Policy on the Prevention of Money Laundering / Combatting Terrorism Financing

and

Know Your Business & Know Your Customer Policy

Contents

1. Introduction and background

This Policy on the Prevention of Money Laundering / Combatting Terrorism Financing and Know Your Business & Know Your Customer Policy (hereinafter referred to as the "AML/KYC Policy", "AML Policy", or the "Policy") applies to RocketFuel A/S, Denmark ("RocketFuel") and aims to prevent and mitigate possible risks of RocketFuel being involved in any kind of illegal activity.

As approved by Authorised Management and the Board of Directors of RocketFuel, this policy applies to all individuals working at all levels within RocketFuel, including senior managers, officers, directors, employees, all external service providers (including consultants), contractors, trainees, homeworkers, part-time and fixed-term workers (all of whom are collectively referred to as "staff").

The AML Policy shall be communicated to all staff and at all times readily accessible, e.g. on the Intranet and/or common drives.

This Policy's main objectives are to:

- Define the principles and measures applied by RocketFuel in the fight against money laundering and terrorism financing ("AML/CFT");
- Provide guidance and clarify the approach and attitude to be adopted when confronted with money laundering or terrorism financing.
- Comply with applicable AML/CFT laws, regulations and standards, including those applicable to fighting corruption as well as to sanctions and embargoes;
- Ultimately, preserve RocketFuel's reputation through limitation and adequate management of AML/CFT risks.

RocketFuel acts as platform provider for merchants and payers/customers to perform crypto-currency payments and instant bank transfers. As a Payment Service Provider, RocketFuel does not at any stage of the payment chain hold user's funds while solely processing payment transactions. RocketFuel will perform in-dept due diligence on Merchants/Payees and Simplified Due Diligence on customers/payees according to Section 5.4 and 5.5.

All the customers have already been through a due diligence process and been approved with either the relevant crypto-currency exchange and/or the Banks, where the customer has a crypto-currency wallet and/or a bank account.

RocketFuel's AML/KYB processes and procedures will be focused on:

Merchants/Payee, Section 5.4.
Such processes and procedures will cover client / merchant / contracting party on-boarding and due diligence, relationship review and transaction monitoring. Measurements and risk assessment tools will assist RocketFuel to on-board and monitor its merchants to prevent and detect any potential money laundering or terrorist financing activities.

Customers/Payers, Section 5.5.
RocketFuel will perform Simplified Due Diligence on the customers side, to minimise risk and any potential money laundering or terrorist financing activities associated with payments via RocketFuel.

2. Company policy

The AML Policy's main objective is to define the principles and measures applied by RocketFuel in the fight against money laundering and terrorism financing, as well as to provide guidance and clarify the approach and attitude to be adopted when confronted with money laundering or terrorism financing, thereby ensuring that RocketFuel adheres to applicable AML laws, regulations and standards, including those applicable to fighting corruption as well as to sanctions and embargoes.

Prevention of money laundering and terrorist financing is essential to protect RocketFuel against legal consequences, financial loss and reputation damage by managing compliance, regulatory and reputation risks actively, mitigating those risks and thereby seeking to prevent, detect and report suspicions of money laundering. RocketFuel intends to offer assurance that RocketFuel does not enter into or maintain business relationships with companies, structures or persons where it suspects, knows or is reasonably expected to know that they have a criminal background or used for financing terrorism.

RocketFuel takes a zero-tolerance approach to money laundering, terrorist activity, and other such financial crimes. Neither commercial considerations nor a sense of loyalty to clients / contracting parties shall be permitted to take precedence over RocketFuel's anti-money laundering commitment.

Reputation damage may seriously impact RocketFuel as it may lead to unwillingness of clients or professional counterparts to initiate or continue their business relationships with us and may lead to fines or constraints on our business activities imposed by regulators or by any other competent authority.

The AML Policy, taking all current regulatory requirements and standards in terms of the fight against money laundering and terrorism financing into consideration, shall evolve and be updated from time to time to reflect legal and regulatory evolution affecting RocketFuel. This Policy shall be subject to regular controls and verifications according to the money laundering and terrorism financing risks to which RocketFuel is exposed.

3. Money Laundering and Terrorism Financing – Definitions and Concepts

3.1. Money laundering

Generally speaking, money Laundering is the process of disguising the origin of the proceeds of crime. Terrorist financing provides funds for terrorist activity. The use of products and services by money launderers and terrorists exposes RocketFuel to significant criminal, regulatory and reputational risk.

More precisely, money laundering can be defined as the processing of criminal proceeds (including but not limited to drug trafficking) to disguise their illegal origin or the ownership or control of the assets, or promoting an illegal activity with illicit or legal source funds. Money laundering is commonly seen as occurring in three steps:

- The first step involves introducing cash into the financial system by some means ("**placement**");
- The second involves carrying out complex financial transactions to camouflage the illegal source ("**layering**");
- And the final step entails acquiring wealth generated from the transactions of the illicit funds ("**integration**").

Some of these steps may be omitted, depending on the circumstances; for example, non-cash proceeds that are already in the financial system would have no need for placement.

Under International law, the money laundering offence is defined as:

a) Knowingly facilitating the false justification of the origin and nature of an activity, or any direct or indirect proceeds or benefit derived from any of the designated predicate offences (i.e. the deliberate falsification, by whatever means, of the source of property constituting the subject of or the direct or indirect proceeds of or some form of pecuniary advantage drawn from one or more of the designated primary offences);

b) Knowingly assisting in a placement, dissimulation or conversion transaction of the activity or any direct or indirect proceeds or benefit derived from one or several predicate offences (i.e. the act of aiding and abetting in the investment, concealment or conversion of property constituting the subject of or the direct or indirect proceeds of or some form of pecuniary advantage drawn from one or more of the designated primary offences);

c) Having acquired, held or used the assets underlying the activity, or the direct or indirect proceeds or benefits of any nature whatsoever from one or several of the predicate offences, knowing, at the time they were received, that they originated from one of the designated offences or from the participation in one or several of these offences (i.e. the act of acquiring, possessing or using property constituting the subject of... in the knowledge at the time of handling that the property originated from committing or taking part in the commission of one or several primary offences).

Money laundering is an offence in its own right, which may be pursued independently from any proceedings or sentences for any of the predicate or primary offences (see definition below). It should also be noted that a money laundering offence is punishable even a) when only attempted, and b) even when the predicate offence was committed abroad.

The financing of terrorism offence is defined under International law as the unlawful and wilful providing or collecting of funds, securities or assets of any type by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out or attempt to carry out one or more offences defined as acts of terrorism.

A predicate (or primary) offence is an offence the subject or proceeds of which may give rise to the money laundering offence, meaning that money laundering presupposes the existence of an underlying (predicate) offence. Under International law, there is a very wide list of predicate offences, including on the one hand infringements specifically indicated as predicate offences (such as some of the ones listed hereunder) and on the other hand an open list of infringements defined according to a level of seriousness comprising all infringements sanctioned by imprisonment of a minimum higher than 6 months. The list of specifically designated predicate offences contains, mainly, the following:

- Trafficking in drugs and psychotropic substances,
- Participating in a criminal conspiracy or in a criminal organization,
- Kidnapping, illegal restraint and hostage taking,
- Sexual exploitation (prostitution and procuring), including sexual exploitation of minors,
- Trafficking in human beings and illicit trafficking in migrants,
- Illicit arms and ammunition trafficking,
- Public and private corruption,
- Abuse of company assets,
- Counterfeiting, piracy, use and disclosure of trade / manufacturing secrets,
- Counterfeiting of coins and banknotes,
- Theft and other crimes against property,
- Insider trading and market manipulation,
- Terrorism or financing of terrorism,
- Aggravated tax fraud and tax evasion.

Certain predicate offences generate direct patrimonial advantages (drug trafficking, abuse of corporate assets, etc.) whereas others generate such advantages only indirectly (forgery, use of forgery, etc.).

3.2. Terrorism Financing

There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well-established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property. More generally:

- Often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;
- Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

3.3. Other definitions

For the purpose of this policy, the following definitions shall apply:

a. “Client” or “Merchant” or “Payee” means contracting party with RocketFuel providing its Payment Processing Services to their customers via RocketFuel.
b. “Customer” or “Payer” means natural person using the RocketFuel Payment Services to pay for a product / service at the ecommerce web shop.

4. Money Laundering Reporting Officer (MLRO) - Role and Responsibilities

RocketFuel designates a senior individual to be the Money Laundering Reporting Officer (MLRO), who is also responsible for RocketFuel's Risk & Compliance function. The MLRO has overall responsibility for the establishment and maintenance of RocketFuel's AML/KYB/KYC framework and underlying systems and controls. The MRLO reports directly to the CEO, as well as to the Board of Director's Risk & Compliance Committee.

RocketFuel ensures the MLRO has sufficient seniority within the company and has the relevant experience and understanding of AML/KYB/KYC to carry out his/her duties. RocketFuel's Authorised Management and Board of Directors fully supports and ensures the MLRO has resources available for his/her role and provides on-going support and development to his/her activities.

The MLRO, with the support of Authorised Management and the Board of Directors, is responsible for ensuring that RocketFuel meets its AML/KYB/KYC requirements in accordance with applicable legislation. The MLRO will oversee the AML/KYB/KYC systems and controls and ensure they are fit for purpose. The main activities of the MLRO comprise, but are not limited to, the following:

- Oversight of all aspects of RocketFuel's AML/KYB/KYC activities;
- Be the focal point for all activities within the company relating to AML/KYB/KYC;
- Provide AML training to all staff;
- Receive all internal suspicious activity reports and, where deemed applicable, report to relevant authorities on the same;
- Be the focal point for law enforcement and other regulatory bodies;
- Establish the basis on which a risk-based approach to the prevention of money laundering and terrorism financing is put into practice;
- Support and coordinate senior management focus on managing the money laundering/terrorist financing risk in individual business areas;
- Advise the business on new products / processes from an AML perspective.

The MLRO is also required to produce reports for the Board of Directors (respectively the Board's Risk & Compliance Board Committee) meetings including, but not limited to, the following items:

- Confirmation that adequate merchant and customer due diligence information is being collected and that on-going monitoring is taking place;
- Summary data relating to complex or unusual transactions;
- Number of internal consents / Suspicious Activity Reports (SARs) received from staff members;
- Number of SARs sent;
- Information on status of staff training within the company;
- Confirmation that all business records have been properly stored and are retained according to regulatory requirements;
- Changes in the law/operating environment which do or might impact the business;
- Changes in the risk matrix affecting the business;
- Contacts with regulators.

5. Know Your Business Policy - AML Risk Assessment

As a matter of principle, RocketFuel shall not knowingly enter into business relationships or participate in activities with persons, legal entities, or structures in connection with money laundering or terrorism financing.

RocketFuel enforces a strict anti-money laundering policy with zero tolerance for money laundering or terrorism financing activities and ensures it knows its customers / clients / merchants / contracting parties and also who it is going into business with. Such activity is more commonly known as due diligence, Know Your Customer (KYC) or Know Your Business (KYB). RocketFuel has set out robust processes and procedures to meet these requirements.

The MLRO is responsible for ensuring an AML risk assessment is completed, regularly reviewed, and updated as part of its overall risk management framework. The risks assessed should help determine the strength of RocketFuel's policies and procedures and control systems in place to help prevent and detect such money laundering or terrorism financing activity.

5.1. Prohibited business relationships and activities

Accordingly, any activity constituting or linked to a predicate offence or bribery of officials is strictly forbidden (see definition of predicate offences above). The following business relationships, whether with persons, companies, or structures, are prohibited where it is known or expected to be known that such relationships are:

- Involved in criminal or terrorist activities, or support criminal or terrorist activities;
- Banks that have no physical presence in the place of incorporation (so-called "shell banks");
- Supporting or carrying out unregulated/regulated money remittance business or unregulated/regulated bank note dealers;
- Prohibited by law or regulation as a result of sanctions and embargoes;
- Classified as unwanted relationships, either in a local or in a global database
- Establishing a business relationship on an anonymous basis or under fictitious names.

RocketFuel has a more detailed "Acceptance Policy" reviewed quarterly.

5.2. Risk-based approach

RocketFuel is committed to assist in the fight against money laundering, including corruption and terrorism financing, by operating an effective risk-based approach. The measures and processes applied by RocketFuel for establishing, monitoring and reviewing business relationships are based on such approach, taking into account legislation and industry guidance as applicable. Risk-based approach standards defined in this Policy should be considered as minimum standards to be applied by all RocketFuel staff.

The MLRO will assess money laundering and terrorist risks presented by:

- Merchant risk – specific categories of merchants and the resulting business relationships;
- Customer risk – risks relating to the potential high-risk nature of the persons;

- Payment risk – payment methods offered and the degree to which their specific characteristics are vulnerable to ML/TF threats;
- Geographical or country risk – the risks posed by geographical or country factors;
- Product risk – products offered and the degree to which their specific characteristics may be attractive for money laundering or financing terrorism;
- Supplier / Third party risk - risks of on-boarding new clients / suppliers and not understanding who owns the business or considering other AML risks;
- Technological Risk – risks with technology used by the company, how susceptible is it to money laundering or terrorist financing;
- Employee risk – the risks posed by employees of the company;
- Regulatory Risk – the risks of non-compliance with license and regulatory frameworks and the risk of penalties to the company and individuals.

5.3. Risk categories

RocketFuel divides its business relationships into three different AML/CFT risk levels (Low, Medium, High) depending on a number of criteria such as a client's domicile, industry or activity, political function or type of transactions. Any business relationship not falling into a Low or High Risk category based on above criteria shall be qualified as Medium, meaning that standard due diligence measures shall be applied. The risk categorisation of a business relationship is triggered either by the contracting partner (natural or legal person, account holder, authorised signatory or proxy holder) or the ultimate beneficial owner (where different from the contracting partner).

Generally, for all of RocketFuel's activities, the following risk categories as defined should determine the risk-based measures and impact client / contracting party risk classification:

a. **Politically Exposed Persons (PEPs) associated with the merchant**

A Politically Exposed Person ("PEP") is a person who is or has been entrusted with a prominent public function, whether residing in US, Europe or abroad, or holding a public function in Europe, US or in a foreign country or holding a public function on behalf of a foreign country. This definition also includes any person identified as being a close family member of or close associate of such public official.

Any RocketFuel business relationship affected by such persons, whether as contracting partner, proxy holder, authorised signatory or ultimate beneficial owner, shall as such be considered High Risk and require specific Risk & Compliance and Authorised Management formal prior approval. The responsible Relationship Manager must re-submit once a year any PEP business relationship for review and approval by Risk & Compliance and Authorised Management.

Examples of prominent public functions include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliament or of similar legislative bodies;
- Members of the governing bodies of political parties;
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;

- Ambassadors, charges d'affaires and high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory bodies of State-owned enterprises;
- Directors, deputy directors and members of the board or equivalent function of an international organisation.

b. **Sensitive Country Affected Business Relationships** (SCAB)

A Sensitive Country Affected Business Relationship ("SCAB") is a High-Risk business relationship where an individual or legal entity has a substantial connection (in the sense of: is domiciled, has a tax residence, is operating in or has close business relations) with any of the countries in Categories 2 to 4 as defined below. Under control of the competent internal acceptance committee, it is the Relationship Manager's responsibility to identify whether such substantial connection exists and consequently classify or not a relationship as High Risk.

Whilst there is no universally agreed definition of how to rate a particular country or geographic area as High Risk, country risk - in conjunction with other risk factors - provides useful information with respect to potential risks of money laundering and terrorism financing. Based on available sources (EU publications, FATF, IMF and Transparency International reports and statements, CSSF Circulars, etc.), countries can be listed in four main categories:

- Countries such as EU/EEA countries or countries with equivalent AML/CFT standards, laws and regulations (Category 1);
- Countries with strategic AML/CFT deficiencies, but having developed an action plan to address such deficiencies (Category 2);
- Countries identified (by the FATF) as lacking appropriate AML/CFT laws and regulations, showing strategic deficiencies or not committed to an action plan to address such deficiencies (Category 3);
- Countries subject to sanctions, embargoes or similar measures (Category 4).

Where countries fall into Category 1, and although there is a general equivalence assumption for EU Member States, Risk & Compliance shall assess, document (based on relevant and up-to-date information) and regularly review whether an EU Member State or a third country imposes AML/CFT obligations equivalent to those imposed under applicable EU Directives laws and regulations. The fact that an EU Member State or a third country is considered as imposing equivalent AML/CFT obligations does not relieve RocketFuel from assessing AML/CFT risks when on-boarding new business relationships or when confronted with High-Risk situations, i.e. applying enhanced due diligence where necessary.

The Risk & Compliance function shall publish from time to time updated lists of sensitive countries according to their AML/CFT risk level per category and append the lists to this Policy (Appendix 2).

c. **Sensitive Industry Affected Business Relationships** (SIAB)

A Sensitive Industry Affected Business Relationship ("SIAB") is a High-Risk business relationship where an individual or legal entity has a substantial connection to a sensitive industry or activity. Under control of the competent internal acceptance committee, it is the Relationship

Manager's responsibility to identify whether such substantial connection exists and consequently classify a relationship as High Risk.
In the context of this Policy, the following main business sectors are to be considered as sensitive industry or activity and is considered prohibited according to RocketFuel's acceptance policy:

- Unlicensed Casinos, betting or other unlicensed gambling related activities;
- Defence, arms or war materials manufacturers and dealers, private military services;
- Diamond and/or precious stones traders / dealers;
- Money remittance businesses and bank note dealers in the non-banking sector;
- Religious organisations;
- Sensitive charities and non-profit organisations;
- Sensitive intermediaries.

The Risk & Compliance function shall review from time to time the lists of sensitive industries according to their AML/CFT risk level per category and amend this Policy and the acceptance Policy, accordingly as need be.

In defining the risk-based approach, RocketFuel shall at least apply following key principles:

- Whilst all business relationships with PEPs shall be categorised per se as High Risk irrespective of any other risk categorisation, all other relationships shall be considered High, Medium or Low Risk in accordance with defined terms for each category.
- Any business relationship qualified as High Risk shall as a matter of principle be submitted to higher on-boarding, due diligence, monitoring and review standards.
- Under US and European law, any business relationship not entered into through face-to-face contact, i.e. remotely, constitutes a higher risk situation requiring appropriate enhanced due diligence measures (see hereunder for further details). In such instance's strict procedures, mechanisms and processes are implemented in order to verify the identity, rights and powers of clients or proxies to access RocketFuel's services.

5.4. Due Diligence and Merchant / Contracting Party Acceptance Processes

Due diligence in relation to clients / contracting parties does not end with the commencement of a business relationship. It is a permanent process primarily performed by the Relationship Manager or client-facing staff throughout the entire period of the relationship.

5.4.1 Business relationship acceptance

Business relationship acceptance within RocketFuel is always subject to a minimum "four-eyes" principle, whereby the detailed acceptance, relationship opening, and on-boarding procedures (including checklists or other forms) are determined in writing and approved by the Risk & Compliance function and Authorised Management. Additional or different acceptance measures, such as enhanced due diligence, approval level or approval by certain functions, shall apply depending on the specific level of risk of a business relationship.

Said procedures shall also cover and adequately document in writing all instances where RocketFuel has not accepted to enter into a business relationship, as well as maintain documentation in accordance with record-keeping requirements.

5.4.2 Client Identification, Identity Verification and Due Diligence

As a general rule before any business relationship is entered into, RocketFuel must in all cases identify and verify the identity of its clients / contracting parties (which includes all proxy holders, authorised signatories and ultimate beneficial owners) on the basis of documents, data or information obtained from a reliable and independent source. RocketFuel must further establish the purpose and intended nature of the business relationship, e.g. the origin of funds.

Merchant Due Diligence

AML Law imposes that a Merchant Due Diligence (hereinafter "MDD") must be applied each time in following instances:

- When establishing a business relationship;
- When there is a suspicion of money laundering or terrorism financing, irrespective of any derogation, exemption or threshold;
- When there are doubts about the veracity or adequacy of previously obtained client identification data.

Performing standard MDD means that, as a minimum, the following four measures are executed:

1. Identification of the client / contracting party and verification of the client / contracting party's identity

For purposes of client / contracting party identification, the following information must at least be gathered and registered, as follows:

1.a. For natural persons in the management, board of directors, and UBOs: surname and first name; place and date of birth; nationality; address; and (where appropriate) official identification number. The verification of identity for natural persons shall be performed by obtaining at least a copy of:

- a valid official identification document issued by a public authority, which document bears the client's signature and picture (e.g. passport, ID card or residence permit) and;
- an address verification document not older than 3 months (e.g. utility bill or bank statement).

Such documents should be clearly legible and reasonably allow recognition of the individual. Client identification and verification of identity also includes the identification (and verification of identity) of proxies.

1.b For legal entities (e.g. limited companies, partnerships, etc.) or legal arrangements (e.g. trusts, foundations, etc.): denomination; legal form; registered office address and (if different) principal place of business; (where appropriate) official identification number; directors or persons exercising similar positions in case of legal

arrangements; authorisation to enter into a relationship (e.g. Board or shareholders resolution). All natural persons involved in the legal person or legal arrangement (be it as director, proxy holder or signatory, etc.) should be identified in accordance with standards set above. All documents obtained must be either originals or certified copies of such originals. The link(s) between all involved persons and/or companies must be made clear.

The verification of identity for legal persons or legal arrangements shall be performed by obtaining at least a copy of the following documents:

- The last coordinated or up-to-date certificate of incorporation (or equivalent document)
- Articles of Association / Memorandum;
- A recent and up-to-date extract from the companies register (or equivalent supporting evidence)
- An up-to-date company structure document
- The documents evidencing that any natural person acting on behalf of legal person or arrangement is properly authorised to do so (power to bind), and his/her identity is verified

In accordance with RocketFuel's risk assessment on the business relationship, the Bank shall take additional verification measures such as:

- Examination of the last management report and the last corporate accounts, where appropriate, certified by an approved statutory auditor
- Verification that the company is not subject to a dissolution, bankruptcy, or liquidation
- Verification of the identification and due diligence information collected from independent and reliable sources (e.g. private or public databases)
- A visit to the company or contacts with the company among others through registered letter with acknowledgment of receipt

2. Identifying, where applicable, the beneficial owner

Verification of client / contracting party and beneficial owner identity must take place before establishing a business relationship or executing a transaction. At such time, the Relationship Manager must determine whether the client / contracting party is acting for his own account or for the account of other persons and to take necessary steps to identify such persons, in which case the client must sign a beneficial ownership declaration as part of account opening process. This requirement includes the obligation to take reasonable measures to verify the beneficial owner's identity using relevant information or data obtained from the client, from public register and/or other independent and reliable sources to satisfy RocketFuel that it knows the true ultimate beneficial owner.

For natural persons, this means the RocketFuel needs to obtain the beneficial owner's surname, first name, nationality, date and place of birth and address, as well as a copy of:

- a valid official identification document issued by a public authority, which document bears the client's signature and picture (e.g. passport, ID card or residence permit) and;
- an address verification document not older than 3 months (e.g. utility bill or bank statement).

Such documents should be clearly legible and reasonably allow recognition of the individual. All documents obtained must be either originals or certified copies of such originals.

For legal persons or legal arrangements, this means that RocketFuel needs to:

- understand the ownership and control structure of the client, and to
- determine who are the natural persons that ultimately own or control the client.

The beneficial ownership of such legal persons or legal arrangements consists of one or several natural persons which ultimately, directly or indirectly, own or control in law or in fact, even if the thresholds of ownership or controls of minimum 25% of the legal person or arrangement as indicated are not met. Such natural persons should then be identified in accordance with standards set above.

When, despite above measures, the Relationship Manager still is in doubt about the real identity of the beneficial owner and where such doubt cannot be dispelled, RocketFuel shall refuse to enter into a business relationship or to carry out the contemplated transaction(s) and, if there is a money laundering or terrorism financing suspicion, apply the Policy as detailed under 7.

3. Obtaining information on the purpose and intended nature of the business relationship

The purpose and intended nature of the business relationship must be established and evidenced by relevant documents and adequate documentation and includes the obligation to gather and register information on:

- The origin of a client's funds, and
- The types of transactions for which he/she requests a business relationship, as well as
- Any adequate information allowing the determination of the client's purpose of the business relationship.

4. Conducting ongoing monitoring of the business relationship

This obligation includes:

- Keeping close scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with RocketFuel's knowledge of the client, its business and risk profile and, where necessary, the source of funds;
- Keeping the documents, data or information held concerning the business relationship up-to-date, as well as keeping records of the findings in respect of such scrutiny covering the background and purpose of said transactions;

- Paying special attention to all complex, unusual large transactions or unusual patterns of transactions having no apparent economic or lawful purpose;
- Paying special attention to transactions significant in relation to the business relationship, transactions that exceed certain limits, very high turnover inconsistent with the size of the balance, or transactions falling out of the regular pattern of the account activity.

5.4.3. Enhanced Merchant Due Diligence

In addition to standard due diligence measures as described above, RocketFuel applies Enhanced Merchant Due Diligence (hereinafter "EMDD") on a risk-sensitive basis, i.e. in situations which by their nature can present a higher risk of money laundering or terrorism financing.

AML Law, European Regulation consider the following as constituting ECDD measures:

- Obtaining additional information on the business relationship and updating more regularly the client and beneficial ownership identification data;
- Obtaining additional information on the intended nature of the business relationship and the reasons for the intended or performed transactions;
- Verifying the additional information obtained with independent and reliable sources;
- Ensuring that the first payment is carried out through an account opened in the client's name with a credit institution according to AML Law or subject to equivalent professional AML/CFT obligations;
- Conducting enhanced monitoring of the business relationship (by increasing the number and timing of controls applied, and selecting transaction patterns requiring further examination).

By law, situations requiring EMDD appear at least in the following instances:

a. <u>Non face-to-face business relationships</u>

Where the client / contracting party has not been physically present for identification purposes (e.g. business relationships entered into, services or transactions concluded remotely over the Internet or via correspondence), RocketFuel implements appropriate policies and effective due diligence procedures when establishing such relationships and conducting ongoing due diligence.

RocketFuel shall take one or more of the following measures to address the specific risks associated with such relationships:

- Ensuring that the client's / contracting party's identity is established by additional documents, data or information;
- Applying supplementary verification or certification of supplied documents, or requiring confirmatory certification by a credit or financial institution governed by European and US AML Law or subject to equivalent AML/CFT professional obligations;
- Ensuring that the first payment of the operations is carried out through an account opened in the client's name with a credit institution according to AML Law or subject to equivalent professional AML/CFT obligations.
- Developing independent contact with the client.

b. Banking relationships

Entering into a business relationship with a US or European bank is subject to prior formal approval of RocketFuel's MLRO and Authorised Management. RocketFuel shall take specific risk-compensating measures, such as:

- Gathering information of the institution with respect to its country of establishment and applicable legal and regulatory provisions in relation to AML/CFT, its supervisory authority and regime, as well as its property and control structure;
- Gathering sufficient information about the financial institution to fully understand the nature of its business and to determine, from publicly available information, the reputation of the institution and the quality of its supervision (including whether the concerned institution has been the subject to a money laundering or terrorism financing investigation or regulatory action);
- Assessing the institution's AML/CFT controls and ascertaining that they are adequate and effective;

Analysis of the obtained information and the resulting assessment on which the decision to enter into a correspondent business relationship was taken shall be documented in writing, reviewed and updated periodically on a risk basis approach. Entering into a banking relationship with a shell bank or banks known to permit their accounts to be used by a shell bank is strictly prohibited.

c. **Transactions or business relationships with PEPs**

Entering into a business relationship with a PEP is subject to prior formal written approval of RocketFuel's MLRO and Authorised Management, after source of wealth and source of funds on the account or involved in the transaction have been thoroughly established and verified. When a client or beneficial owner of an existing business relationship subsequently becomes or is found to be a PEP, the responsible Relationship Manager shall obtain formal approval as indicated above. Identification of business relationships involving a PEP shall normally be ensured through merchant screening as described below. Furthermore, enhanced ongoing monitoring of the business relationship must be performed by the responsible Relationship Manager and reinforced control measures applied (e.g. prior Risk & Compliance approval for all transactions, full due diligence review on a yearly basis).

d. Business relationships with clients from or in countries not applying or insufficiently applying equivalent AML/CFT measures

Business relationships and transactions whether with natural or legal persons or with financial institutions from or in a country which does not apply or applies insufficiently equivalent AML/CFT measures (i.e. those countries defined as falling under Categories 2 to 4 described above) must require special attention and be subjected to ECDD measures, both in acceptance and ongoing monitoring of such relationships or transactions (e.g. prior formal written approval of RocketFuel's Authorised Management and of the Chief Risk & Compliance Officer).

5.4.4. Client / Contracting Party Screening

As a matter of principle before entering into a business relationship, all new clients (i.e. be it physical persons, companies or other entities, corporate directors, beneficial owners, holders of full or limited powers of attorney, authorised signatories) must be screened as minimum against available tools, internal and/or external databases as determined by Risk & Compliance Business relationship screening shall also be performed on all of RocketFuel's service providers.

The screening process is primarily designed to highlight and isolate new high-risk business relationships and/or financial transfers to/from PEP's or persons associated with sanctions or terrorism financing. Existing clients should also be screened as part of recurring risk-based relationship reviews. Any potential "hits" and/or negative news should be (risk-based) investigated to determine whether they relate to the individual or entity being screened, and the outcome of such process must be recorded.

RocketFuel makes use of an external service provider to screen merchants against recognised Sanctions Lists and Politically Exposed Persons (PEPs) lists. Individuals will be screened on on-going basis as well as on initial on-boarding. RocketFuel applies state-of-the-art due diligence tools such as Web Shield "InvestiGate" to ensure the highest quality of the due diligence procedure and the accompanying documentation when on-boarding new merchants. For any live merchant, the Company will use Web Shield's "Monitor" to perform automated and monthly, quarterly, bi-yearly or annual monitoring of all websites associated with the merchant.

Information leading to "fuzzy matches" will be investigated further, for example where the match was related to a name which can be deemed as popular, and this will be compared against the other information that is collected at point of registration. The full evaluation of the merchants data will provide a result.
Any confirmed matches to sanctions lists will be declined or closed, and the necessary reports will be made to the Risk & Compliance function and treated in accordance with AML suspicion requirements as described this Policy.

5.4.5. Basic Client / Contracting Party Documentation

The account opening documentation, together with any required identification information as well as any required identification verification and due diligence documents, forms the basis of a business relationship between RocketFuel and a client /contracting partner. A business relation may thus as a matter of principle only be entered into and opened (i.e. transactions executed and/or services rendered) once all necessary documentation has been correctly signed and completed, required documents have been provided and required internal approvals obtained. Said required documentation shall be determined (e.g. by way of checklists, guidance notes) for each type of business relationship within the applicable approved on-boarding process.

A KYB profile must be established for each business relationship, obtaining and recording detailed and meaningful information on the background, professional activity of the client /

contracting partner and/or beneficial owner. For companies or other corporate structures such detailed information shall include the business sector, type of business, products and services offered as well as the regions and/or markets covered. RocketFuel must further record the purpose and intended nature of the business relationship to be established. The exact contents and details of said client profile are determined within the applicable approved on-boarding process.
In instances where there are deficiencies with respect to the basic required documentation, such exceptional cases must be adequately managed, and remediation monitored.

5.4.6. Client KYB Monitoring and Reviews

Existing business relationships must be continuously monitored and periodically reviewed in accordance with their level of risk. Accordingly, the identification process and the merchant due diligence shall be repeated if, during the relationship, reason is given to doubt the accuracy, completeness or plausibility of the information, or if there are signals of unreported changes.

5.4.6.1. Relationship Monitoring

RocketFuel must create, implement and maintain an appropriate control framework to monitor all business relationships under its responsibility. Said control framework shall constitute a mandatory part of each Business Line's key policies and procedures.

Ongoing due diligence of a business relationship includes scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with RocketFuel's knowledge of the client, its business, its risk profile and the source of his funds. It also includes keeping KYB information (documents, data, information) up-to-date. Due diligence in relation to RocketFuel's clients / contracting parties does not end with the commencement of the business relationship, as it is an ongoing process throughout the entire period of the relationship (e.g. changes in relation to the ultimate beneficial ownership, update of the client profile, etc.). This means that the Relationship Manager(s) must either renew the documentation if need be (e.g. beneficial owner declaration) or update in writing the KYB information in the client / contracting party file. The KYB profile must at all times contain detailed, meaningful information on the client, i.e. contracting party(ies), power(s) of attorney and ultimate beneficial owner(s) as the case may be, such information detailing in particular his/her professional activities, financial situation, or - for companies - the products and services offered and the geographical sales markets.

The ongoing monitoring requirement further means that all relevant complex and unusual large transactions or unusual transaction patterns, e.g. having no apparent economic or lawful purpose, must be identified by the Relationship Manager(s) and monitored on a continuous basis. The background and purpose of relevant transactions must be scrutinised, the findings recorded in writing and documentation kept in accordance with record-keeping requirements. Such transactions involving increased legal, compliance and reputation risks could be described as significant transactions relative to a business relationship, transactions that exceeds certain limits, very high account turnover inconsistent with the size of the balance or transactions which fall out of the regular pattern of the account's activity. The criteria to take into consideration could be:

a. The importance of the incoming and outgoing assets and the volume of the amounts involved (including small amounts, but unusually frequent);
b. The differences compared to the nature, volume or frequency of the transactions usually carried out by the client (or differences compared to transactions normally carried out in the framework of similar relationships);
c. The differences compared to the declarations made by the clients during the on-boarding process, in particular with respect to the purpose and nature of the business relationship, especially the origin and destination of funds.

It is part of the Relationship Manager's professional duties to ensure that the transactions processed for their clients / contracting party are plausible and do not raise suspicions in terms of money laundering or the financing of terrorism. In case of doubt, Relationship Managers must inform the Risk & Compliance function. Relationship Managers are always required to clarify the economic background and the purpose of a transaction, if needed with the support of the Risk & Compliance function, if the transaction appears unusual and/or if there are indications that the assets are the proceeds of crime, or a criminal organisation has power of disposal over the assets.

If it is not possible to consider an unusual transaction as plausible on the basis of the KYC information available in the client / contracting party file, the Relationship Manager must obtain a detailed explanation as well as necessary supporting evidence from the client account holder and/or ultimate beneficial owner or other involved parties. A pending transaction identified as unusual may only be executed once appropriate and acceptable justification is available in the client file.

Relationship Managers must immediately contact the Compliance function in case of doubt, and especially in the following situations:

- Refusal or undue delays from the account holder and/or contracting partner and/or ultimate beneficial owner to cooperate with investigations and/or to provide the requested documentation (plausibility test);
- The additional information provided does not appear plausible;
- The Relationship Managers are alerted by indications of money laundering or financing of terrorism.

5.4.6.2. Special monitoring on the coupons and the Buyer

As a matter of principle, all transactions, will always be associated to a specific purchase and a unique transaction ID.

Moreover, in order to be able to correlate every coupon sold on the RocketFuel's website with the respective buyer, every coupon will be issued with a dedicated serial number which will be recorded in the Transaction ID information at the time of the purchase.

Therefore, for each coupon purchased on the RocketFuel platform; RocketFuel will be able to gather all the information related to this coupon, i.e: transaction ID (date, time, amount of the purchase, cardholder name and email address and IP address)

On top of this, after each purchase, a notification email is being sent automatically to the buyer with the coupon information (serial number) to confirm he has effectively received the gift card, and that the amount has been deposited on the website where the buyer is willing to use the coupon on.
This will allow RocketFuel to ensure that the coupons won't be used anonymously to purchase illegal services/products, as RocketFuel is capable of linking each coupon to each buyer.

By way of giving a unique reference to each voucher, and thus allowing to identify each buyer separately, it will also help RocketFuel to prevent smurfing/transactions structuring.
Indeed, numerous transactions with low amount can be a sign of transaction structuring attempt. Once such behaviour is flagged by the monitoring team, RocketFuel is then able to analyze the information of each flagged transactions, and based on all the elements of this transaction (transaction date and time, amount, IP address, cardholder details, user's email address,…) establish whether it is link to a smurfing attempt or if these low amount transactions are legitimate.

For further information on this, please refer to the "RocketFuel Coupons Workflow" document.

5.4.6.3. Relationship Reviews

All existing business relationships must be reviewed periodically by RocketFuel, applying the approved risk-based approach. The frequency and level of review by the Relationship Manager will depend on the risk categorisation and is determined within applicable procedures. Higher risk relationships should however be reviewed as a minimum standard on a yearly basis.
Any material change in the risk classification standards - i.e. a country newly rated by FATF as non-cooperative or submitted to sanctions, an industry newly rated as sensitive, a business relationship becoming a PEP or the a business relationship falling under a sanction regime - should as such trigger a review of all affected business relationships by all concerned Business Lines, respectively the Relationship Manager. Such material changes will usually be communicated by Legal & Compliance.

Business relationship reviews should be clearly documented and as a minimum include:

- An updated screening check against available tools, databases and the Internet;
- Ensuring existing due diligence information is up-to-date and correctly recorded;
- Ensuring proper understanding and evidencing of transactions conducted by the client / contracting party, including any significant or unusual transactions;
- Conducting further investigations and obtaining further information as may be warranted by new issues or findings.
- Such reviews may further be initiated because of a "trigger" event or unusual transaction.

The Risk & Compliance function will independently monitor RocketFuel's business relationships and conduct its own formal periodic KYB reviews and/or further in-depth reviews on selected (groups of) business relationships, with a focus on high risk relationships, in order to identify any systematic weaknesses or root causes and suggest appropriate mitigating measures.

5.5. End-User Due Diligence and Anti-Fraud Measures

5.5.1 Risk Factors

5.5.1.1. Customer Risk Factors

RocketFuel facilitates payments from payer (end customer) to payee (merchant).

When using the RocketFuel services, Customers/payers must accept RocketFuel's Terms & Conditions and RocketFuel's Privacy Policy. Both RocketFuel's Terms and Condition and Privacy Policy are available on RocketFuel's homepage: www.RocketFuelblockchain.com

RocketFuel performs a Due Diligence (DD) on all merchants and does not onboard merchants from jurisdictions with higher ML/TF risk.

5.5.1.2. Distribution Channel Risk Factors

RocketFuel cannot meet with payers in person to verify their identity, therefore Simplified Due Diligence (SDD) is performed within the checkout page, including a form of identity verification.

5.5.1.3. Country or geographical Risk Factors

RocketFuel performs a due diligence on all merchants and does not onboard merchants from jurisdictions with higher ML/TF risk. Payee account information is configured in the merchant's web shop by RocketFuel during merchant integration phase.

All merchants RocketFuel onboards are required to have a bank account in an EEA member country, to which they shall receive payments, RocketFuel's core business is low risk for this fact.

5.5.2 Measures

RocketFuel does not provide accounts to payers, nor hold funds during any time of the transaction.

5.5.2.1. Business Types

RocketFuel maintains lists of business activities it considers to be within three risk categories: low, medium, and high risk. RocketFuel take a risk-based approach when screening payers at checkout. Different merchant categories carry their own risks associated with their business.

5.5.2.2. Low Risk Business Activity List

Retail, E-commerce, , Manufacturing, Handcrafting, Wholesale

5.5.2.2. Medium Risk Business Activity List

Ticketing, Cruise lines, Hotels, Marketing Services, SEO, AdWords, Online Marketing for licensed gaming operators, Media Consulting services, Legal Services, IT Solutions, Software Development, Business and Management Consultancy, Building Materials and supply, Architectural design activities related to architect projects

5.5.2.3. High Risk Business Activity List

Crypto currency exchange, Forex, Casino, Online Gambling and Gaming, Offline Casinos, PSPs, Adult, Precious stones, Subscription based services, online chat or personal line, nutraceuticals or supplements, credit counselling or repair, Travel and Airlines.

5.5.2.4. Restricted and Prohibited Business Activity List

RocketFuel onboards merchants based on the RocketFuel "Acceptance Policy".

5.5.3 Customer Due Diligence and Anti Fraud Measures

RocketFuel performs a Simplified Due Diligence (SDD) on all transfers.

Typical data that are monitored to detect customer risk includes:

- User ID
- IP address
- Email address
- Phone number
- Device ID / signature
- Purchase History
- User's crypto-currency address
- User's Bank / Bank Account
- Billing address
- Shipping address

Additionally, each payment is verified against a series of anti-fraud checks:

- Fraud Scoring – This score is created for each transfer based on several fraud indicators. Factors include business risk categories, location, sales channel, etc. Fraud scoring generates a risk indication
- Device Fingerprinting – If fraud is detected on a device, this device may be blocked from making any future purchases. Device fingerprinting creates a unique profile of every payer device to identify previously encountered devices
- Geolocation – If the payer is connecting via an IP address that does not match with the customer data, it could indicate a risk of unauthorized use of payment
- Proxy Piercing – Fraudsters may mask their true IP with a proxy to by-pass a geolocation trigger. Proxy piercing sees through this
- Velocity Checking – Multiple purchases made from the same account or to the same address is another indicator of possible fraud. If the same customer pays from different payment accounts over a short period of time, it may be an indicator of a fraud attack.
- Blacklists & Whitelists – RocketFuel blacklists all countries on sanctioned lists, countries with bans on merchant industries, or from known fraudsters.
- Address Verification - RocketFuel compares the billing address provided by the payer against the address on-file with the customer's bank. If the addresses do not match, it raises a red flag

- Machine Learning – algorithms use payment data to find fraud patterns specific to the industry or merchant in question. Over time, with additional data, this become more accurate and faster at detecting fraud than any other fraud tools available. Machine learning will be used to monitor customer behaviour after an initial purchase.
- Biometrics – RocketFuel uses tokenization together with 2Factor authentication. This may be in the form of fingerprinting or other biometric verification.

5.5.3.1. Enhanced Due Diligence

For high risk businesses anti-fraud tools will be used to a stricter degree, and with a lower tolerance.

5.5.3.2. Simplified Due Diligence

If a red flag is raised for possible fraud during a payment RocketFuel will – dependent on risk score – :

1) Send it to manual review, until manually approved.
2) inform the merchant and may decide to block future transfers from payer,
3) ask for further payer KYC documentation prior validating the payment

RocketFuel holds contacts with payee, or merchant, in all cases. The merchant is the client of RocketFuel, and payers are the customers of the merchant. RocketFuel onboards merchants based on RocketFuel Acceptance Policy. The nature of the business relationship is always evaluated in the process of merchant onboarding.

In that sense, RocketFuel will ensure that the merchant products/services offered are done in accordance with local laws and schemes rules. This will be emphasized on an ongoing educational basis. More specifically for high risks businesses, RocketFuel will educate the merchants (fraud tools they use, KYC performed on their end users based on their business) in order to mitigate risks and ensure proper due diligence from their end as well.

Overall, the end-user will go through due diligence and anti-fraud checks at various stages: merchant level, RocketFuel level, and ultimately the end-user's own bank. All this will significantly decrease the fraud risk in this payment landscape.

6. Obligation to Cooperate with Competent Authorities

All of RocketFuel's employees, directors and officers have a duty to cooperate comprehensively and quickly with European authorities competent for the fight against money laundering and financing of terrorism. This cooperation requirement does not end with the business relationship or the transaction.

In practice, this means that RocketFuel has a duty to inform the European authorities in the following circumstances:

a. **Upon request** issued by the authorities responsible for the fight against money laundering and the financing of terrorism, RocketFuel is obliged to quickly and comprehensively provide all

requested information as well as any relevant existing document on which the requested information is based. Such request tends to determine whether RocketFuel is or was in business relationship with, or whether transactions are being or were carried out in relation to specific persons, including persons in relation to certain sensitive countries, or subject to prohibitions or restrictive measures. Above-mentioned requests, indicating the legal basis upon which they are made, are usually addressed in writing by the Public Prosecutor to RocketFuel 's Chief Risk & Compliance Officer.

b. Cooperation with authorities is mandatory **without delay, spontaneously on its own initiative**, when RocketFuel (i.e. its employees, directors and officers) knows, suspects or has good reasons to suspect the possibility that money laundering or financing of terrorism is taking place, took place, or was attempted, in particular by reason of the person(s) concerned, his/her/their evolution, the origin of the assets, the nature, finality or the modality of the operation. A suspicion may thus arise by reason of a fact, in relation to the person concerned, to his development or the origin of his funds, and/or a transaction, in relation to the nature, the purpose or procedures of a transaction. In any case of suspicion and without legally qualifying the facts under criminal law, RocketFuel is legally bound to file a Suspicious Activity Report ("SAR") with the FIU, using the standard required form. Also, as soon as a suspicion of financing of terrorism arises, RocketFuel has a duty to file a SAR irrespective the existence of any money laundering offence and even if the origin of funds is perfectly legitimate. Insofar as there are indicators or suspicions of money laundering or terrorism financing, the duty to inform also covers instances where RocketFuel came into contact with natural or legal persons or entered into a legal arrangement without entering into a business relationship or carrying out a transaction.

   In the context of terrorism financing, the reporting obligation applies to funds for which there a reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist associations, organisations or groups or by those who finance terrorism, without limiting this reporting obligation solely to funds of persons listed by the United Nations or the European Union in the context of terrorism financing.

7. Measures to be taken in the event of a Suspicion of Money Laundering or Terrorism Financing

There is no obligation for RocketFuel to actively seek for evidence of money laundering, neither to seek if such evidence is sufficiently conclusive to be used as a basis for a money laundering or financing of terrorism transaction nor whether conditions for an incrimination are met, neither to qualify the facts, nor to prove their exactitude, as all of this is the task of the competent judicial and prosecuting authorities. It is however the legal duty of every RocketFuel employee, director or officer to immediately report to RocketFuel 's Risk & Compliance function any information or transaction that comes to their attention in the course of their business activities which may qualify as a suspicion under this instruction.

Whenever any RocketFuel staff member, director and/or officer has knowledge, suspicion or reasonable grounds to suspect, or becomes aware at any stage (prospecting or existing relationship) that money laundering or financing of terrorism is being or has been committed, or attempted, in particular in connection to persons, assets or transactions, they must immediately report such information / remit any documentation to the Risk & Compliance function.
Failure to report or unjustifiable delay in reporting a suspicious situation or relationship may lead:

- Internally, to disciplinary action imposed on RocketFuel staff member(s) by RocketFuel 's Authorised Management;
- Externally, to fines or criminal sanctions imposed on individual persons (e.g. RocketFuel staff) and/or RocketFuel itself by the competent authorities.

In order for the Risk & Compliance function to perform all necessary investigations to analyse the situation and determine the need to file a Suspicious Activity Report ("SAR") or in order to respond to a information request from a competent authority, full and immediate cooperation of all RocketFuel staff is required, among others by giving speedy, full unrestricted access to and/or copies of relevant records of the suspected relationship(s) or operation(s). The results of such investigations and analyses shall be recorded in writing and kept by the Risk & Compliance function.

The Risk & Compliance function must also immediately be contacted in the following situations:

- Whenever a client / contracting partner refuses to cooperate with RocketFuel 's investigations;
- If the additional information provided by the client / contracting partner is neither plausible nor credible.

7.1. Money laundering indicators

The obligation to report suspicious transactions applies for each fact that may be an indication of money laundering or financing of terrorism. Indications of money laundering or of a connection to a terrorist or other criminal organisation may arise prior to entering into a business relationship or within the context of an existing business relationship. In such instances additional clarifications must be made and the Risk & Compliance function must be contacted.

A list of money laundering indicators can be found in Appendix 3. Outlined indicators cannot be considered as exhaustive (or in certain cases not entirely applicable to RocketFuel's specific activities), but merely seek to raise awareness and provide assistance to RocketFuel staff in identifying money laundering or terrorism financing transactions. They constitute potential suspicious elements requiring further close attention and investigation, and do not correspond to laundering the proceeds of a specific predicate offence. A single indicator or a doubtful transaction is not necessarily in itself sufficient ground for suspecting a money laundering or financing of terrorism transaction as, in practice, the combination of several indicators or suspicious transactions, the nature of the transactions, the surrounding circumstances or the type(s) of persons involved may be indicative of a money laundering activity.

7.2. Measures to be taken

RocketFuel is expected to take appropriate measures to detect money laundering or terrorism financing indicators whether the relationship is an existing one or whether RocketFuel has not yet formally entered into a business relationship.

7.2.1. Prior to entering a business relationship

Should entering a business relationship not be pursued or be terminated due to potential money laundering issues after a first personal contact (be it written or oral) was established, then RocketFuel employee must immediately inform the Risk & Compliance function and hand over all relevant information and documents collected. The Risk & Compliance function will analyse the information and documents received in order to assess whether a SAR must be filed with the Public Prosecutor or not. There is however no duty to undertake further investigations (economic background, purpose of the relationship, etc.) if the entering into a business relationship is rejected from the very beginning purely for commercial reasons.

7.2.2. In the context of an existing relationship

If any RocketFuel staff member becomes aware of indicators such as those mentioned in this Policy in the context of an existing relationship, he/she must immediately inform the Risk & Compliance function. The plausibility of a client's explanations regarding the background of transactions indicative of a money laundering offence must be assessed by the employee, together with the Risk & Compliance function as need be. It is important to recognise that any explanation provided by the client cannot necessarily be accepted at face value. Particular risks of money laundering are inherent in transactions, of which the structure suggests and illegal purpose, when the economic background cannot be determined or when the transaction appears absurd from an economic point of view.

In deciding whether potential suspicious activity is being undertaken, RocketFuel employees should have a clear understanding of the legitimate business of their merchants. The merchant due diligence information obtained at the outset of and during the merchant relationship plays a vital role in this process. RocketFuel staff should take particular care when the proposed merchant is not well known or is engaged in transactions which are not typical for the merchant or the type of merchant or are unusual from a commercial point of view especially where the transaction is to be settled in an unusual manner. Screening of transactions and of merchants can assist in identifying potential suspicious activity.

RocketFuel staff have a duty to closely monitor with enhanced attention any business relationship which was the subject of a suspicion report to the FIU, in accordance as the case may be with specific instructions from the FIU as communicated by the Risk & Compliance function to the employee. In case of new AML/CFT indicators or suspicions, the employee must immediately notify the Risk & Compliance function, as a complementary SAR must then be filed.

7.3. Sending a SAR to the MLRO

The standard process for sending a SAR to the MLRO requires the RocketFuel staff member to send an email from his/her personal work email address to compliance@RocketFuelblockchain.com with “SAR submission” as the subject line.

Said email should provide at least following information:

- client(s) / contracting party(ies)’s name(s);
- system references, where applicable;
- any reference to the transaction / amount;
- a brief explanation of the staff member’s reasons for suspicion, adding any email or other relevant information on the activity (even If the suspicion relates to a third party / supplier).

The designated RocketFuel MLRO will send an acknowledgement of the staff email. The Risk & Compliance Officer will then review the suspicion report and determine how best to proceed (including advice on how to proceed with the involved parties) and whether to submit a SAR to the FIU.

7.4. Filing a suspicious activity report

A decision on whether a SAR is to be filed with the FIU rests with the MLRO, whereas the concerned RocketFuel staff member, Manager and Authorised Management will be informed of and involved as need be in the process. Until such decision is taken, no further transaction can be made or service performed.

The MLRO shall file a SAR with the FIU in accordance with applicable guidelines and procedures (through the GoAML tool).

Whenever a SAR is filed:

- The Public Prosecutor can block one or more relationships or suspicious transactions. Such instruction is communicated in writing to RocketFuel 's Risk & Compliance function and is normally valid for an initial maximum period of 3 months (which may be prolonged each time for another period of 1 month, up to a maximum total period of 6 months). The Public Prosecutor has no authority to authorise a transaction or in relation to a suspicious person, but has the power to block execution of such transaction.
- The Public Prosecutor may wish to be kept informed of any new developments / transactions with respect to one or more relationships, even if the account(s) is(are) not or have never been blocked.

All notified accounts / relationships remain blocked by the Risk & Compliance function until the Public Prosecutor has given relevant instructions or confirmed in writing that the case is closed.

7.5. Tipping off prohibition

There is a strict prohibition on tipping off. RocketFuel staff are strictly prohibited to inform directly or indirectly any client, contracting partner, account holder, proxy holder, beneficial owner or any other party connected that information has been communicated to the FIU, or that a money laundering or financing of terrorism investigation is in process (irrespective of whether RocketFuel initiated a suspicion report or the authorities issued a formal request). This is a personal criminal offence under European and US law. In the event a client / contracting partner wants to execute a transaction which has been blocked by the Public Prosecutor, the Risk & Compliance function must be contacted immediately.

All communication between staff and the client(s) from that point on needs to be handled with care, the Risk & Compliance will provide advice as to how to handle such situations.

8. Employee training

Employee training with respect to AML/KYC matters is ensured in accordance with principles defined and under responsibility of the Risk & Compliance function within RocketFuel.

Basic principles of AML Training at RocketFuel are defined as follows:

- New employees joining RocketFuel shall, within 3 months of entry, be required to go through the AML training provided and pass the tests contained therein;
- As a standard refresher course, all current RocketFuel staff shall go through the AML training, on a yearly basis;
- The RocketFuel Risk & Compliance Officer is responsible for keeping track and recording attendance to such trainings.

All employees will be made aware, through an annual compulsory training programme, of:

- The risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation;
- RocketFuel's procedures covering how to recognise and deal with potential money laundering or terrorist financing suspicious transactions or activity;
- The identity and responsibilities of the RocketFuel's nominated MLRO (the Risk & Compliance Officer).

9. Record keeping

All of RocketFuel's departments must, as a minimum, keep records of all client identification and transaction data, account files, as well as of the relevant documents, business correspondence and information obtained under the due diligence measures, including the results of any performed analysis, including client screening (PEPs & Sanctions), as applied according to this Policy.

The supporting evidence and records of business relationships and transactions must consist of the original documents or certified copies in accordance with European and US law. In order to permit reconstruction of individual transactions (so as to provide as the case may be evidence for prosecution of criminal activity), such transaction records must provide client identifying information normally recorded by RocketFuel, nature and date of the transaction, type and amount of currency, as well as type and identifying number of any account involved in the transaction.

Any archiving medium may be used for record-keeping purposes, provided the documents meet the conditions for said documents to be used as evidence in a judicial procedure or investigation or analysis of money laundering and terrorism financing by any AML/CFT competent authority.

This record-keeping obligation is valid for a period of at least five years following the carrying out of a transaction or the termination of an account or business relationships, without prejudice of any longer record-keeping periods prescribed by European and US law.

10. Sanctions

Failure to comply, infringements (including circumvention) of this Policy and associated policies may result in disciplinary proceedings, which could ultimately lead to dismissal.

All questions regarding this Policy will be answered by the below contact person(s).

Document Owner	Contact Details
Name:	Ben Yankowitz
Position:	Head of Risk and Compliance
Email	b.yankowitz@rocketfuelblockchain.com

Appendix 1 - Essential US, European and international regulatory reference texts

Further key European and international regulatory reference can be found in the following documents:

- (5th AML Directive) EU Parliament and Council Directive 2018/843 of 30 May 2018, amending EU Directives 2015/849, 2009/138 and 2013/36, on the prevention of use of the financial system for the purpose of money laundering and terrorist financing (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN)
- (4th AML Directive) EU Parliament and Council Directive 2015/849 of 25 May 2015, amending Regulation 648/2012 and repealing Directive 2005/60/EC and Commission Directive 2006/70/EC, on the prevention of use of the financial system for the purpose of money laundering and terrorist financing (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN)
- EU Parliament and Council Directive 2018/1673 of 23 October 2018 on combating money laundering by criminal law (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN)
- EU Parliament and Council Directive 2014/42/EU of 3 April 2018 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0042&from=EN)
- EU Parliament and Council Regulation 2018/1672 of 23 October 2018 on controls on cash entering or leaving the Union, repealing Regulation (EC) No 1889/2005 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1672&from=EN)
- EU Council Regulation 2018/1542 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1542&from=EN);
- EU Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN);
- Standards, Guidance Papers and Recommendations issued and updated from time to time by the European Banking Authority (EBA -), the Financial Action Task Force (FATF - www.fatf-gafi.org), as well as Global AML standards and statements published by the Wolfsburg Group (www.wolfsburg-principles.com).

Appendix 2 - List of Sensitive Countries

RocketFuel is exclusively doing business with companies/merchants with HQ and official address in a European country. However, some beneficial owners could have address in countries outside Europe, and we will not accept any merchant having CEO's, signatories or beneficial owners with addresses in the following countries categorized under the Financial Action Task Force (FATF) and the European commission Directive (EU) 2015/849, Article 9, as high-risk countries;

Afghanistan
Albania
American Samoa
Bahamas
Barbados
Botswana
Cambodia
Democratic People's Republic of Korea (North Korea)
Ethiopia
Ghana
Guam
Iran
Iraq
Jamaica
Libya
Mauritius
Mongolia
Myanmar
Nicaragua
Nigeria
Pakistan
Panama
Puerto Rico
Samoa
Saudi Arabia
Sri Lanka
Syria
Trinidad and Tobago
Tunisia
Uganda
US Virgin Islands
Yemen
Zimbabwe

Appendix 3 - Indicators of potential money laundering and/or terrorism financing

This annex provides a list of indicators likely to reveal a possible laundering of a predicate tax offence to the professionals of the financial sector subject to the supervision of the Financial Supervisory Authorities in US.

If an indicator or a combination of indicators raises doubts, RocketFuel staff members must examine the business relationship/transaction more thoroughly in order to verify if doubts are justified given the context of the transactions and RocketFuel's knowledge of the client / contracting party's situation

There are numerous indicators that may act as "red flags" for RocketFuel staff in identifying potential money laundering or terrorism financing activity. Although a single indicator does not necessarily indicate illicit activity, the existence of a "red flag" indicator should encourage further monitoring and examination by any RocketFuel staff member. In most cases it is the existence of multiple indicators that raises the RocketFuel's suspicion of potential criminal activity, and influences the response to the situation. Money launderers and terrorism financiers will continuously look for new techniques to obscure the origins of illicit funds to give the appearance of legitimacy to their activities.
Risk & Compliance will ensure that these money laundering/terrorism financing indicators are included in staff training and encourage employees to use these indicators when describing suspicious behaviours for inclusion in suspect transaction or suspicious activity reports.
The list below features "red flag" indicators that RocketFuel staff members should familiarise themselves with. This list should be treated as a non-exhaustive holistic guide for educational purposes and not applicable per se to RocketFuel since several indicators do not apply as such to Payment Service activities.

General Red Flags

- Account activity inconsistent with merchant profile
- Account operated by someone other than the owner
- Betting accounts with large deposits but minimal betting activity
- Business activity inconsistent with business profile
- Cash payments for funds transfer
- Cash withdrawals from betting account in cheques and vouchers
- Client is a known frequent gambler and/or high roller at a casino
- Client purchases or sells real estate above or below market value while apparently unconcerned about the economic disadvantages of the transaction
- Co-mingling of illicit funds with legitimate sources of income
- Company account used for personal use
- Frequent cash deposits made over a short period of time
- Frequent cheque deposits
- Funds transfers involving a tax haven
- Multiple transfers occurring on the same day to the same beneficiary
- Numerous large deposits via ATMs
- Outgoing transfer with corresponding incoming funds transfer or 'U-turn' transactions
- Purchase of bank cheques
- Purchase of bank drafts by third parties
- Purchase of high value assets
- Same day transactions at different geographical locations
- Same home address provided for funds transfers by different people
- Structuring of funds transfers of transactions
- Third parties used to open bank accounts
- Transactions inconsistent with merchant profile

- Unusual merchant behaviour
- Use of cash couriers
- Use of company accounts for personal use
- Use of false company
- Use of false identification documentation
- Use of false invoices
- Use of family member accounts
- Use of gatekeepers (e.g. accountant. Lawyer, etc.)
- Use of inactive account
- Use of multiple accounts for deposit
- Use of third parties to conduct international funds transfers
- Use of third parties to conduct transactions
- Use of third party accounts
- Use of variation when spelling names/addresses

Red Flags about the client / contracting party

- The client is overly secret or evasive about who he is, who the beneficial owner is, where the money is coming from, or why they are doing a certain transaction in this way,
- The client is using an agent or intermediary without good reason,
- The client is actively avoiding personal contact without good reason,
- The client is reluctant to provide or refuses to provide information, data and documents usually required in order enable the transaction's execution,
- The client holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics involved,
- The client provides false or counterfeited documentation,
- The client is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact,
- The client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals,
- The client is or is related to or is a known associate of a person listed as being involved or suspected of,
- The client is using multiple bank accounts or foreign accounts without good reason,
- Private expenditure is funded by a company, business or government,
- An unusually short repayment period has been set without logical explanation,
- The asset is purchased with cash and then rapidly used as collateral for a loan,
- The company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, with no logical explanation,
- The creation of complicated ownership structures when there is no legitimate or economic reason,
- Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason,
- There is an absence of documentation to support the client's story, previous transaction, or company activities,
- Abandoned transactions with no concern for the fee level or after receipt of funds,
- There are unexplained changes in instructions, especially at the last minute,
- There is a lack of sensible commercial/financial/tax or legal reason for the transaction,
- There is increased complexity in the transactions, or the structures used for the transaction which results in higher taxes and fees than apparently necessary,

- A power of attorney is sought for the administration or disposal of assets under conditions which are unusual, where there is no logical explanation,
- Requests for payments to third parties without substantiating reason or corresponding transaction.

Red Flags about predicate tax offences

- The merchant is a legal person or a legal arrangement set up in a jurisdiction that is not subject to AEOI/CRS/FATCA reporting and this "entity" has no economic, asset or other reality, except where (1) the merchant demonstrates that its establishment complies with the legal provisions of the country of residence of the merchant /beneficial owner or (2) the existence of the entity is in effect known to the tax authorities of the country of residence of the beneficial owner based on supporting evidence.
- The merchant is a company or uses companies in which a multitude of statutory changes (unexpected and short-term changes) have taken place, for example with the purpose of appointing new managers, moving the registered office to a jurisdiction which is not subject to AEOI/CRS/FATCA reporting, amending the corporate purpose or corporate name, not justified by the economic situation of the company.
- The use of companies or legal structures located in a jurisdiction other than the tax residence or place of regular economic or professional interests of the beneficial owner, except where (1) the merchant demonstrates that its establishment complies with the legal provisions of the country of residence of the merchant /beneficial owner or (2) the existence of the legal person is in effect known by the tax authorities of the country of residence of the beneficial owner based on supporting evidence.
- Completion of a commercial transaction at a price that is obviously under-estimated, over- estimated or inconsistent.
- Findings of anomalies in the documentation justifying the transactions, and notably atypical or unusual transactions (e.g. *no VAT number, no invoice number, no address, all of which may put into question the supporting evidence of the document supplied*).
- The merchants refusal to provide the tax compliance documentation or information needed for tax reportings or the presence of indications raising suspicions regarding fiscal non- compliance.
- Substantial increase, over a short period, of movements on banking account(s) which was (were) until then scarcely active or inactive, without this rise being justified, notably by a verified development of economic or business activities of the merchant.
- Observation of inconsistencies between the business volume (e.g. based on company accounts) and movements on bank accounts.
- Substantial and/or irregular transactions linked to professional activities on personal/private accounts.
- Payment or reception of fees to or from foreign companies without business activities or without substance or link between the counterparties and whose purpose seems to be economically unjustified re-invoicing.
- Classification of a company or legal structure as "Active Non-Financial Entity" based on CRS regulations and without the change being justified by the development of the business of the company or legal structure.
- Requests for assistance or provision of services whose purpose could be to foster circumvention of the merchant's tax obligations.
- Use by the merchant of complex structures without economic or asset purpose, except where e.g. (1) the merchant demonstrates that its establishment complies with the legal provisions of the country of residence of the merchant/beneficial owner or (2) the existence of the legal person is in effect known by the tax authorities of the country of residence of the beneficial owner based on supporting evidence.

- Unjustified refusal of any contact or unjustified request of hold mail and more particularly if the merchant is domiciled in a jurisdiction that is not subject to AEOI/CRS/FATCA reporting (e.g. *the unjustified request of a merchant not to be contacted ever in writing (post and/or e- mail); the merchant states that tax obligations are fulfilled and has signed a tax compliance statement, but has never collected its post or consulted its account online. The merchant does thus not have the necessary elements to fulfil its tax obligations*).
- The transfer of funds from a country that according to the professional could be considered as being risky from a tax transparency point of view, except for example where the merchant provides evidence that the funds have been declared.
- Inconsistent information available to the professional concerning the tax residence of the merchant.
- Use of so-called back-to-back loans, without valid justification.
- Move of the tax residence from a jurisdiction that is not subject to AEOI/CRS/FATCA reporting to a jurisdiction that is subject to such reporting without notifying the professional, in order, potentially, to escape reporting.
- Financial transactions that are inconsistent with the usual activities of the merchant or with its profile or with the asset situation stated by the merchant or suspect operations in sectors that are prone to VAT or other tax fraud, in a generally cross-border context.
- Withdrawal or deposit of cash that is not justified by the level or nature of the commercial activity or known professional or asset situation.
- Documentation on tax compliance leaving room for doubt as it was issued by a person close to the final merchant and there being a potential conflict of interests.

Policy Review and Maintenance

Change History

Issue Number	Issue Date	Details on the Changes
v1.1	February 2021	Approved
V1.2.	July 2021	Approved
V1.3	January 2022	Approved
V1.4	July 2022	Approved
V1.5	January 2023	Approved

Who to contact to if you have any queries, questions, changes, or concerns?

Document Owner	Contact Details
Name:	Ben Yankowitz
Position:	Head of Risk and Compliance
Email	B.yankowitz@rocketfuelblockchain.com