The Website (https://rival.finance/) and Mobile Application are owned by the company RIVAL PAYMENTS SERVICES PROVIDER LLC, incorporated in United Arab Emirates with a registered number 1308095 and registered office at Dubai, Business Bay, Burlington Tower, Office 403.

Cryptocurrency services offered on the Website and Mobile Application are provided by UAB Choise Services. UAB Choise Services is incorporated in Lithuania with the company number 305964183, registered office at Vilnius, Eišiškių Sodų 18-oji g. 11. UAB Choise Services is registered as a virtual currency exchange operator and a custodian virtual currency wallet operator. UAB Walletto (registration number 304686884) is authorized by the Bank of Lithuania to conduct electronic money service activities under the Law on Electronic Money and Electronic Money institutions (license number 33).

Digital currency values are not static and fluctuate due to market changes. Not all products and services are available in all geographic areas and are subject to applicable terms and conditions. We do not provide services to citizens of the Russian Federation, or non-EU residents. Eligibility for particular products and services is subject to final determination by Choise Services UAB. Rates for products are subject to change.

Last updated: 1st March 2024

Rival Finance Anti-Fraud Policy

1. Introduction

The Anti-Fraud Policy (the **“AF Policy”**) of RIVAL PAYMENTS SERVICES PROVIDER LLC, incorporated in United Arab Emirates with a registered number 1308095 and registered office at Dubai, Business Bay, Burlington Tower, Office 403 **("Rival Finance")** and Choise Services UAB ("**Company**", "**Choise**", "we" or "us") is established to prevent and mitigate possible risks of Choise Services UAB being involved in illegal or illicit activities and to enable Choise Services UAB to meet its legal and regulatory obligations in this area (if any, where applicable). This AF Policy is subject to changes and updates by Choise from time to time to ensure compliance with any applicable legislation and global AF practices.

Therefore, Choise Services UAB is regulated and compliant with the laws and regulations to combat money laundering and terrorist financing:

- Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania
- Order of FCIS Director No. V-240 on approval of “Money laundering and suspicious monetary operations or transactions recognition criteria list”
- Order of FCIS Director No. V-129 on the approval of “Recommendations for the information submission forms, submission scheme, and filling of submission forms according to the requirements of the Law on the prevention of money laundering and terrorist financing”
- Order of FCIS Director No. V-5 issued 2020-01-10 on the approval of “Instructions for deposit network operators to prevent money laundering and/or terrorist financing “
- Order of FCIS Director No. V-129 on the approval of “Recommendations for the information submission forms, submission scheme, and filling of submission forms according to the requirements of the Law on the prevention of money laundering and terrorist financing”
- Recommendations for Money Laundering of FATF

2. Policy Statement

2.1. Choise will comply with the applicable laws of Lithuania. In line with applicable laws, Choise has a ‘zero tolerance’ policy towards fraud, collusion, money laundering, financing of terrorism, and other criminal conduct and will thoroughly investigate and seek to take legal action against those who perpetrate, are involved in, or assist with fraudulent or other improper actions in all Choise activity and related transactions.

2.2. Choise will provide adequate and appropriate resources to implement the Anti-Fraud Policy and will ensure it is communicated and understood.

3. Purpose&Scope

3.1. The purpose of this document is to outline the responsibilities of all the involved parties concerning fraud prevention, the actions to be taken if fraud is suspected the mechanism of verifying suspicion of fraud, the reporting process, and the recovery action plan.

4. Legislation Compliance

4.1. The Anti-Fraud Policy has been drafted to comply with the currently applicable law, including, but not limited to applicable laws of Lithuania.

4.2. Adherence to the Anti-Fraud Policy Choise will ensure compliance with all relevant legislation and internal policies.

5. The User verification

5.1. The User undertakes to provide Choise with correct and relevant personal information and documents contained therein. In case the User provides counterfeit documents and false personal information, such behavior will be interpreted as fraudulent activity.

5.2. The User hereby authorizes Choise, directly or indirectly (through third parties, including Crypterium AS), to make any inquiries as we consider necessary to check the relevance and accuracy of the information provided for verification purposes. Personal Data transferred will be limited to strictly the necessary and with security measures in use to protect the data as specified in our Privacy Policy.

6. Account Security

6.1. The User is responsible for maintaining the confidentiality of their Account's credentials, including, but not limited to a password, email, wallet address, balance and of all activity including transactions made through the Account.

6.2. If the User has any security concerns about his/her Account, login details, password or other security feature being lost, stolen, misappropriated, used without authorization or otherwise compromised, the User is advised to change the password. The User must contact us via support@rival.finance without undue delay on becoming aware of any loss, theft, misappropriation or unauthorized use of the Account, login details, password or other security features. Any undue delay in notifying Choise may not only affect the security of the Account but may result in the User being liable for any losses as a result.

6.3. Any loss or compromise of the User's electronic device or the User's security details may result in unauthorized access to the User's Account by third parties and the loss or theft of any digital currency held in the User's Account. The User must always keep his/her security details safe. For example, User should not write them down or otherwise make them visible to others.

6.4. The User should never allow remote access or share his/her computer screen with someone else when the User is logged on to the Account. Choise will never under any circumstances ask the User for IDs, passwords, or 2-factor authentication codes, screen share or otherwise seek to access the computer or Account. User should not provide details to any third party for the purposes of remotely accessing User's Account unless specifically authorized.

6.5. Choise assume no responsibility for any loss that the User may sustain due to the compromise of Account login credentials due to no fault of Choise.

7. Key Responsibilities

7.1. In view of the Anti-Fraud Policy Choise is responsible for:

- Undertaking a regular review of the fraud risks associated with each of the key organizational objectives;

- Establishing an effective anti-fraud response plan, in proportion to the level of fraud risk identified;
- The design of an effective control environment to prevent fraud;
- Establishing appropriate mechanisms for:
  - reporting fraud risk issues.
- Making sure that all staff are aware of Choise Anti-Fraud Policy and know what their responsibilities are in relation to combating fraud; and
- Ensuring that appropriate action is taken to minimize the risk of previous frauds occurring in the future.

8. Fraud detection and investigation

8.1. Choise ’s Operational Anti-Fraud Department, in particular, the Head of Anti-Fraud Services, is the first line of detection, investigation, and protection in preventing Prohibited Activities through the Users and transactions appraisal process. The Head of Anti-Fraud Services will be responsible for the proper fulfillment of the Anti-Fraud Policy.

9. Miscellaneous

9.1. Choise will review the Anti-Fraud Policy to reflect new legal and regulatory developments and ensure good practice.

Introduction

The following terms and conditions ("**Terms**") are an agreement between you and Card Issuer that governs your access to and use of your Card through Apple Pay. By registering to add Card for use in Apple Pay on your Apple Devices, or allowing another cardholder to add a Card linked to your Card Account for use in Apple Pay on their Apple Devices, you agree that you have read, understood, and accepted all of the Terms contained herein and to use your Card in accordance with these Terms. If you do not agree with any of the following Terms, you must cease all access to, or use of your Card in connection with, Apple Play and/or remove any Card linked to your account from Apple Pay.

These Terms shall be read in conjunction and in addition with the Terms and Conditions of Payment Cards ("**Agreement**") which are available at https://vault.rival.finance/ and associated with Card. It is important that you read these Terms and the Agreement together. In the event of any inconsistency between the provisions of these Terms and the Agreement relating to your access to or use of Card through Apple Pay, the provisions of these Terms shall prevail.

You also acknowledge that your use of Apple Pay is subject to the terms and conditions set forth by Apple with respect to the use of Apple Pay, which will not change or override these Terms.

Eligibility / Enrollment

Apple Pay is available to Card cardholders for the purposes of purchasing goods and services with an eligible Apple Device at near field communication ("**NFC**") enabled merchants and/or an online merchant, who accepts Apple Pay as a form of payment.

To add your Card to Apple Pay, you must register your Card through Apple Pay via application or by directly scanning or entering the Card details manually on Apple Pay wallet ("**Apple Pay Card Registration**"). You may be required to take additional steps to authenticate yourself before your Card is added to Apple Pay, including providing the correct one-time password ("**OTP**") which will be sent to you by us via SMS on your registered mobile number with us ("**Additional Authentication**"). Your enrolment will be declined if the Card is not eligible for this service, you failed the authentication process, or if your Card or the underlying Card Account is not in good standing or conducted in a proper or satisfactory manner as determined by us at our absolute discretion. Apple Pay may also limit the number of Cards that you may store in a single Apple Device from time to time which we cannot control. We may, however, limit the number of Apple Devices in which the same Card can be stored from time to time and you should refer to our latest communications regarding such limit.

For a Program Account which contains multiple Cards issuance, each Card shall be regarded as separate, and thus be subject to a separate Apple Pay Card Registration and Additional Authentication individually.

By adding your Card to Apple Pay, a unique numerical identifier different from your Card number ("**Device Card Number**") will be allocated for the purpose of making purchases and

receiving refunds through Apple Pay. Due to the manner in which Apple Pay operates, you may need to present your Apple Device at a merchant when you return an item purchased using Apple Pay on such Apple Device.

Once a Card is added to Apple Pay, you can use Apple Pay to authorise transactions on a Card Account. This is done by using the relevant Apple Device in place of a Card at a contactless payment terminal or in an application on an Apple Device.

Renewal of your Card upon expiry or replacement of the damaged Card will not affect your use of the same Card enrolled for Apple Pay, whether or not you have activated the renewed or replacement Card.

Your use of Cards through Apple Pay

You must keep your Apple Device safe or secure, by locking it when not in use or when it is unattended and/or by installing up-to-date anti-malware or anti-virus software on it (wherever applicable), including ensuring that the device is not modified contrary to the software or hardware guidelines of the manufacturer or intentionally disabling the device's hardware or software controls (commonly referred to as "jailbreaking"). You acknowledge and agree that the use of a modified device to use your Card in connection with Apple Pay is expressly prohibited and constitutes a violation of these Terms, and is grounds for us to deny your access to your Card through Apple Pay.

You must also ensure that your passcode or personal identification number that is required to allow you to use your Apple Device to access and use your Cards to make purchases through Apple Pay is kept secure in the same way as a cardholder would for a banking password or PIN, including but not limited to, by:

- Not disclosing or sharing to any one;
- Not carrying a record of it with an Apple Device or anything liable to be stolen with an Apple Device (unless a reasonable effort is made to protect the security of the device);
- Not choosing an easily guessable passcode such as the cardholder's date of birth or a recognisable part of the cardholder's name; and
- Not acting with negligence in failing to protect the security of the passcode.

You must take all steps and prevent any fraud, loss or theft in respect of your Apple Device or any of your Card in connection with the use of Apple Pay.

If biometric identifiers are registered on your Apple Device and are used to identify you or be used to grant access to and use your Card for Apple Pay, you must not save a third party's biometrics such as fingerprint (biometric information) on the device. In the event a third party's biometrics are saved on the device, whether now or in the future, and such biometric details can be used to grant access to the device to access and use your Card, you understand, acknowledge and agree that you will be taken to have authorised that person to transact on your behalf and the relevant transactions will be charged to your Card, to which you shall be responsible and liable for the same.

If you enrol for biometric verification such as fingerprint identity ("**Touch ID**"), personal identification number or passcode on Apple Pay, the collection, storage, enrolment and access to Apple Pay using your biometric information, personal identification number or passcode will be made using the technology on your Apple Device. Accordingly, when you log into Apple Pay and choose to be verified using the technology on your Apple Device, your fingerprint or any other biometric information, personal identification number or passcode will be matched and verified against your device's technology. Accordingly, you acknowledge that we have no control over the technology on the Apple Device, the availability, capability, verification method, security and integrity of the Apple Device and cannot be held responsible for transactions effected using Apple Pay and authorized using any biometric information or personal identification number or passcode. You should therefore assess if the Apple Device's manner of verification and risks associated with such use is acceptable to you.

The use of Apple Pay is at your own discretion. You are not obliged to use Apple Pay in connection with any of your Cards. Accordingly, you agree that the access and use of your Card on Apple Pay will be considered as authorized by you and you shall be responsible and liable for the same. If you share your passcode with any other person, you are taken to have authorized that person to transact on your account using Apple Pay. This means that any Apple Pay transaction initiated by that person using the fingerprint or passcode will be authorized by you and the clauses of the Agreement which deals with unauthorized transactions will not apply. If your Apple Device is lost or stolen, any biometric information or personal identification number or other passcode is compromised or used or your Card has been used through Apple Pay without your permission, you must notify us immediately and if we so require, furnish to us a statutory declaration in such form as we specify and/or a police report and/or any other information we may reasonably require. You are liable for all unauthorized use of your Card in connection with Apple Pay until you notify us unless we determined, at our sole discretion that: (i) you have fully complied with these Terms (including, but not limited to the safety precautions) and you notified us without delay, (ii) you assist in the investigations and recovery, and (iii) we are satisfied that such unauthorized transactions are not due to your wilful misconduct and/or gross negligence and that you have not acted fraudulently.

You agree and acknowledge that the transaction history displayed in Apple Pay in connection with the use of your Card in Apple Pay solely represents our authorization of your Apple Pay transaction using that particular Apple Device and does not reflect any post authorization activity, including but not limited to clearing, settlement, foreign currency exchange, refunds, returns or chargebacks.

Accordingly, the purchase amount, currency, and other details for your Apple Pay transaction history in connection with use of your Card in Apple Pay may not match the transaction amount that is ultimately cleared, settled, and posted to your Card statement of account. If there is any inconsistency between your Card statement of account and transaction history displayed in Apple Pay, your Card statement of account shall prevail, and you will remain liable to us for the amounts set out on your statements.

Fees and charges
All applicable fees, interests and charges that apply to your Card pursuant to the Agreement are available and provided on our website and will continue to apply after you have registered your Card with Apple Pay. We currently do not impose any additional fees for using your Card through Apple Pay but we reserve the right to impose a fee at our sole discretion in the future. You shall be solely responsible for all third-party charges, such as your telecommunications carrier or provider may impose web-enablement, data usage or text messaging fees and/or other charges associated with your use of Apple Pay.

As a condition of using your Card in connection with Apple Pay, you acknowledge and consent to us sending notifications and automatically dialled calls or text messages to the Apple Device which may or may not be the same device as your mobile phone number on record with us.

Suspension and Termination of Apple Pay
We have the right to suspend, block or cancel your ability to use your Card in connection with Apple Pay at any time and need not give you any prior notice or reason for doing so, including, modifying or suspending the type of transactions allowed on your Card in connection with Apple Pay, change the eligibility of a Card for use with Apple Pay, and/or change the Card authentication process.

We also have the right to impose a limit on any daily and/or individual transaction amount(s) charged to your Card through Apple Pay. The limit will be at such amount(s) as determined by us and notified to you from time to time.

In the event we have cancelled or suspended your Card in accordance with these Terms and/or the terms of the Agreement, you will not be allowed to use it through your Apple Device. Please note that this is the case even though you may still see a symbol for the Card on your Apple Device.

Authorization to collect and share data
You agree that we may collect, transmit, store, and use technical, location, and login or other information about you and your use of your Card through Apple Pay. We may also collect information relating to your Apple Device (including app version, device type and model, operating system and security information such as whether you have obtained root access):

- To ensure your Card properly functions in Apple Pay;
- For security purposes and to identify fraud;
- For Reap to better provide assistance to you; and
- To tell you about other products or services that may be of interest to you.

You acknowledge that (i) Apple, the provider of Apple Pay technology that supports your Card in Apple Pay, as well as its subcontractors, agents, and affiliates, and (ii) the applicable payment network branded on your Card (i.e., Visa) as well as subcontractors, agents, and affiliates of such payment networks, will have access to certain details of your transactions made with merchants via use of your Card through Apple Pay in and/or for the purposes of

(1) performing its obligations hereunder; (2) providing you with relevant transaction data; (3) detecting and addressing fraud; (4) complying with applicable laws and regulations; (5) responding to inquiries made pursuant to court orders or by regulators; (6) managing, making product enhancement to, and/or promoting the use of Apple Pay; and (7) creating business and/or technical performance reporting. You acknowledge that the use, storage and disclosure of any personal information provided by you directly to Apple, the applicable payment network branded on your Card (i.e., Visa), or other third parties supporting Apple Pay, will be governed by the privacy policy of such party.

Merchant relationships and disclaimers

Merchants may present to you certain discounts, rebates or other benefits (e.g. free shipping) ("**Offers**") if payment is effected through Apple Pay. Such Offers are subject to certain terms and conditions between you and the relevant merchant. We will not be liable for any loss or damage as a result of any interaction between you and a merchant with respect to such Offers. All matters, including delivery of goods and services, returns, and warranties, are solely between you and the applicable merchants. You acknowledge that we do not endorse or warrant the merchants that are accessible through Apple Pay or the Offers that they provide.

Changes to Terms and Conditions

We may amend at any time these Terms, by providing reasonable prior notice to you. We may revise these Terms at any time by updating this posting. You are bound by such revisions and should therefore visit our website to review the current Terms from time to time.

Intellectual Property

All intellectual property rights including all patents, trade secrets, copyrights, trademarks and moral rights (collectively, "**Intellectual Property Rights**") in Apple Pay (including text, graphics, software, photographs and other images, videos, sound, trademarks and logos) are owned either by Apple, us, our licensors or third parties. Nothing in these Terms gives you any rights in respect of any intellectual property owned by Apple, us, our licensors or third parties and you acknowledge that you do not acquire any ownership rights by adding your Card to, or using your Card in connection with, Apple Pay.

Apple, Apple Pay are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

Disclaimers of warranty

Apple Pay is provided by Apple, and without warranty from us. You acknowledge and agree that from time to time, your use of the Card in connection with Apple Pay may be delayed, interrupted or disrupted for an unknown period of time for reasons we cannot control. Neither we nor our affiliates will be liable for any claim arising from or related to use of your Card through Apple Pay due to such delay, interruption, disruption or similar failure.

You acknowledge that we are not party to the terms and conditions for Apple Pay between you and Apple and we do not own and are not responsible for Apple Pay. We are not providing any warranty for Apple Pay. We are not responsible for the performance, maintenance or other support services for Apple Pay and shall not be responsible for any

other claims, losses, liabilities, damages, costs or expenses with respect to Apple Pay, including, without limitation, any third party product liability claims, claims that Apple Pay fails to conform to any applicable legal or regulatory requirement, claims arising under consumer protection or similar legislation, and claims with respect to intellectual property infringement. Any inquiries or complaints relating to the use of Apple Pay, including those pertaining to Intellectual Property Rights, should be directed to Apple.

We do not recommend, endorse or make any representation or warranty of any kind regarding the performance or operation of your Apple Device. You are responsible for the selection of an Apple Device and for all issues relating to the operation, performance and costs associated with such Apple Device.

Limitation of liability

To the maximum extent permitted by applicable law, in no event shall we, our processors, suppliers, or licensors (or their respective affiliates, agents, directors, and employees) be liable for any direct, indirect, punitive, incidental, special, consequential, or exemplary damages, including without limitation damages for loss of profits, goodwill, use, data, or other Intangible losses, that result from the use of, inability to use, or unavailability of Apple Pay, including your use of Card in connection with Apple Pay.

To the maximum extent permitted by applicable law, we, our processors, suppliers, and licensors (and their respective affiliates, agents, directors, and employees) assume no liability or responsibility for any (i) errors, mistakes, or inaccuracies of content; (ii) personal injury or property damage, of any nature whatsoever, resulting from your access to or use of Apple Pay, including your use of your card in connection with Apple Pay; (iii) any interruption or cessation of transmission to or from Apple Pay; (iv) any bugs, viruses, Trojan horses, or the like that may be transmitted to or through Apple Pay by any third party; (v) any errors or omissions in any content or for any loss or damage incurred as a result of the use of any content posted, emailed, transmitted, or otherwise made available through Apple Pay; and/or (vi) user content or the defamatory, offensive, or illegal conduct of any third party.

Indemnity

You will indemnify, defend, and hold us (and our employees, directors, agents, affiliates and representatives) harmless from and against any and all claims, costs, losses, damages, judgments, tax assessments, penalties, interest, and expenses (including reasonable attorneys' fees) arising out of any claim, action, audit, investigation, inquiry, or other proceeding instituted by a person or entity that arises out of or relates to: (a) any actual or alleged breach of your representations, warranties, or obligations set forth in these Terms, including any violation of our policies; (b) your wrongful or improper use of Apple Pay, including wilful misconduct or fraud; (c) your violation of any third-party right, including without limitation any right of privacy, publicity rights or Intellectual Property Rights; (d) your violation of any law, rule or regulation of Hong Kong or any other country; (e) any access or use of Apple Pay by any other party with your Touch ID or personal identification number or passcode or other appropriate security code, and (f) any change in law, regulations, guidelines or official directive or circulars which has an effect on the Card or Apple Pay, and the same may be debited to your Card and/or shall be paid by you on demand.

Representation and warranty
You represent and warrant to us that: (i) to the extent you identified a name at registration, the name identified by you when you registered your Card to be added to Apple Pay is your name; (ii) you are the cardholder of all Cards you add to Apple Pay; (iii) you and all transactions initiated by you or using any of the Cards added to Apple Pay will comply with all laws, rules, and regulations applicable to you, including any applicable tax laws and regulations; (iv) you have the authority to authorize the receipt of notices, calls and text messages from us at the phone number you provide, (v) you will not use any of your Card through Apple Pay for any fraudulent undertaking or in any manner so as to interfere with the operation of Apple Pay; (vi) you will not permit any use of your Card through Apple Pay by any third party; and (vii) your use of your Card in connection with Apple Pay will comply with these Terms.

Removal of your Card from Apple Pay
You shall follow the instructions from Apple Pay to remove your Card from Apple Pay if you no longer wish to use your Card through Apple Pay. You should also ensure that any Card is removed from your Apple Device before the disposal of such Apple Device. Removal of your Card from Apple Pay will not terminate your Card unless you also choose to terminate such in accordance with the terms of the Agreement.

Severability
If any provision or part of a provision of these Terms is illegal, invalid or unenforceable, it will be severed from these Terms and the remaining provisions (or parts of provisions) will continue in full force and effect.

Governing Law
The same laws that govern the Agreement shall govern these Terms.

Definitions
In these Terms, all capitalised words or expressions used shall be defined and carry the same meaning as stated in the Definition section of the Terms and Conditions of Payment Cards ("**Agreement**") except for the following words defined below:

"**Apple Device**" means any devices that supports any of the operating systems released by Apple (e.g., iOS, MacOS, watchOS etc.), which Reap determines, at its sole discretion, is eligible for the registration of Card to be used in Apple Pay. Any devices that are modified contrary to the software or hardware guidelines of the manufacturer, including by disabling hardware or software controls (commonly referred to as "jailbreaking"), are not eligible for the registration of Card to be used in Apple Pay.

"**Apple Pay**" means the mobile payment and digital wallet service created by Apple that lets users make payments using certain devices which support the operating systems released by Apple and credit cards or debit cards registered on such Apple Devices.

“**Card Issuer** “, “**Reap**”, “**we**” or “**us**” means Reap Technologies Limited and its subsidiaries.

“**You**” means the Company of the Program Account related to the Card which has been added to the Apple Pay digital wallet on any Apple Device and, as the context requires, includes any relevant Authorized User.

Last updated: 1st March, 2024

Cookie Policy

Our website https://rival.finance/ (the “Website”) uses cookies to distinguish you from other users of our Website. This helps us to provide you with a good experience when you browse our Website and also allows us to improve our Website. By continuing to use our Website, you are agreeing to our use of cookies.

This Cookie Policy provides you with information on the use of cookies on our Website. It supplements our Privacy Policy which may be accessed at the Website.

Any questions or concerns relating to the use of cookies by our Website and the processing of personal data obtained through their use may be directed to: legal@rival.finance

1. Cookies – What are They and How Do We Use Them?

As is common practice with almost all professional Websites this site uses cookies, which are tiny files that are downloaded to your computer, to improve your experience. A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer’s hard drive. You block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of the Website.

The Website uses cookies to recognize you and your preferences, enhance the performance of our Website, and collect analytical information for the benefit of our customers. The term cookies include similar technologies for collecting and storing information, such as Local Shared Objects (commonly referred to as "flash cookies") and web beacons or web bugs (including transparent or clear gifs).

Session cookies allow us to track your actions during a single browser session, for example, to remember the items returned from a search. They do not remain on your device beyond your session.

Persistent cookies remain on your device between sessions and allow us to authenticate you and to remember your preferences.

The table below explains the types of cookies we use on our Website and why we use them.

Category of cookies	**Why do we use these cookies**
Strictly Necessary	These cookies are essential for Website on our services to perform their basic functions. These include those required to allow registered users to authenticate and perform account-related functions.

Performance	They allow us to recognize and count the number of visitors, track views of content, and see how users move around the Website when they are using it. This helps us to improve the way the Website works, for example, by ensuring that users are finding what they are looking for easily.
Targeting	These cookies record your visit to the Website, the pages you have visited, and the links you have followed. We will use this information to make the Website more relevant to your interests. We may also share this information with third parties for this purpose. For example, we use Google Analytics which uses cookies and similar technologies, to collect and analyze information about the use of the Services and report on activities and trends. This service may also collect information regarding the use of other Website, apps, and online resources.
Third Party / Embedded Content / Other	These include social media Website such as Facebook and Twitter (through the use of sharing buttons), or embedded content. As a result, cookies may be set by these third parties, and used by them to track your online activity. We have no direct control over the information that is collected by these cookies.

From time to time we test new features and make subtle changes to the way that the site is delivered. When we are still testing new features, these cookies may be used to ensure that you receive a consistent experience whilst on the site whilst ensure we understand which optimizations our users appreciate the most.

For more general information on cookies see the Wikipedia article on HTTP Cookies.

2. Managing Cookies. Disabling Cookies

You may choose to change your cookie preferences by clicking on the “Customise Cookies” link. You may not disable any cookies that are strictly necessary through our Website.

If you wish to opt out of all cookies (including necessary cookies) and delete any cookies that have already been placed for this Website and any other Website, you can do this through your browser settings. Your browser's 'help' function will tell you how to do this. However, please remember that cookies are often used to enable and improve certain functions on our Website. If you choose to switch certain cookies off, it is likely to affect how our Website works. Please note that by deleting or blocking cookies that are strictly necessary for the performance of our Website, it may not function correctly and you may not be able to access certain areas of the Website.

You can prevent the setting of cookies by adjusting the settings on your browser (see your browser Help for how to do this). Be aware that disabling cookies will affect the functionality of this and many other Website that you visit. Disabling cookies will usually result in disabling certain functionality and

features of this site. Therefore it is recommended that you do not disable cookies.

3. **The Cookies We Set**

- **Site preferences cookies**

To provide you with a great experience on this site we provide the functionality to set your preferences for how this site runs when you use it. To remember your preferences we need to set cookies so that this information can be recalled whenever you interact with a page that is affected by your preferences.

- **Third-Party Cookies**

In some special cases, we also use cookies provided by trusted third parties. The following section details which third-party cookies you might encounter through this site. This site uses Google Analytics which is one of the most widespread and trusted analytics solutions on the web to help us understand how you use the site and ways that we can improve your experience. These cookies may track things such as how long you spend on the site and the pages that you visit so that we can continue to produce engaging content. For more information on Google Analytics cookies, see the official Google Analytics page.

Third-party analytics are used to track and measure the usage of this site so that we can continue to produce engaging content. These cookies may track things such as how long you spend on the site or pages you visit which helps us to understand how we can improve the site for you.

4. **Links to Other Sites**

The Website´s Website may contain links to other sites that are not owned or controlled by the Website. Please be aware that the Website is not responsible for the privacy or security practices of such other sites. We encourage you to be aware when you leave our site and to read the privacy statements of every website that collects personally identifiable information

5. **Google Analytics**

Our Website uses Google Analytics, a web analysis service provided by Google Inc. ("Google"). Google Analytics works using cookies. Google Analytics cookies collect your IP address; however, because IP anonymization is used on this Website, your IP address will be shortened (and therefore anonymized) as soon as technically possible and before it is stored or otherwise used in connection with Google Analytics. We use the information collected by Google Analytics cookies to find out about how visitors use our Website. Google will not combine the IP address sent by your browser in connection with Google Analytics with other data. You can prevent Google Analytics cookies from being stored by setting your browser software accordingly. You can also opt out of Google Analytics by downloading and installing the browser plug-in available at google.com.

6. Other Information

Retention of data

We retain personal data collected using cookies needed for personalized services where you have consented to the use of cookies for those purposes. You can read more about how we process personal data generally by taking a look at our Privacy Policy.

Your rights

If you are an EU resident, you have certain rights about any personal data that we process about you.

Updating of Cookie Policy

If we change the cookies we use, we will update this Cookies Policy. We reserve the right to make changes to our Cookie Policy from time to time. You always can find the latest version of this Cookie Policy on our Website.

Introduction

The following terms and conditions ("**Terms**") are an agreement between you and Card Issuer that governs your access to and use of your Card through Google Pay. By registering to add Card for use in Google Pay on your Android Device, or allowing another cardholder to add a Card linked to your Card Account for use in Google Pay on their Android Device, you agree that you have read, understood, and accepted all of the Terms contained herein and to use your Card in accordance with these Terms. If you do not agree with any of the following Terms, you must cease all access to or use of your Card in connection with, Google Play and/or remove any Card linked to your account from Google Pay.

These Terms shall be read in conjunction and in addition with the Terms and Conditions of Payment Cards ("**Agreement**") which are available at https://vault.rival.finance/ and associated with each Card. It is important that you read these Terms and the Agreement together. In the event of any inconsistency between the provisions of these Terms and the Agreement relating to your access to or use of Card through Google Pay, the provisions of these Terms shall prevail.

You also acknowledge that your use of Google Pay is subject to the terms and conditions set forth by Google with respect to the use of Google Pay, which will not change or override these Terms.

Eligibility / Enrollment

Google Pay is available to Card cardholders for the purposes of purchasing goods and services with an eligible Android Device at near field communication ("**NFC**") enabled merchants and/or an online merchant, who accepts Google Pay as a form of payment.

To add your Card to Google Pay, you must register your Card through Google Pay via application or by directly scanning or entering the Card details manually on Google Pay wallet ("**Google Pay Card Registration**"). You may be required to take additional steps to authenticate yourself before your Card is added to Google Pay, including providing the correct one-time password ("**OTP**") which will be sent to you by us via SMS on your registered mobile number ("**Additional Authentication**"). Your enrolment will be declined if the Card is not eligible for this service, you failed the authentication process, or if your Card or the underlying Card Account is not in good standing or conducted in a proper or satisfactory manner as determined by us at our absolute discretion. Google Pay may also limit the number of Cards that you may store in a single Android Device from time to time which we cannot control. We may, however, limit the number of Android Devices in which the same Card can be stored from time to time and you should refer to our latest communications regarding such limit.

For a Program Account which contains multiple Cards issuance, each Card shall be regarded as separate, and thus be subject to separate Google Pay Card Registration and Additional Authentication individually.

By adding your Card to Google Pay, a unique numerical identifier different from your Card number ("**Device Card Number**") will be allocated for the purpose of making purchases and receiving refunds through Google Pay. Due to the manner in which Google Pay operates, you

may need to present your Android Device at a merchant when you return an item purchased using Google Pay on such Android Device.

Once a Card is added to Google Pay, you can use Google Pay to authorise transactions on a Card Account. This is done by using the relevant Android Device in place of a Card at a contactless payment terminal or in an application on an Android Device.

Renewal of your Card upon expiry or replacement of the damaged Card will not affect your use of the same Card enrolled for Google Pay, whether or not you have activated the renewed or replacement Card.

Your use of Cards through Google Pay

You must keep your Android Device safe or secure, by locking it when not in use or when it is unattended and/or by installing up-to-date anti-software on it (where applicable), including ensuring that the device is not modified contrary to the software or hardware guidelines of the manufacturer or intentionally disabling the device's hardware or software controls (commonly referred to as "jailbreaking"). You acknowledge and agree that the use of a modified device to use your Card in connection with Google Pay is expressly prohibited and constitutes a violation of these Terms, and is grounds for us to deny your access to your Card through Google Pay.

You must also ensure that your passcode or personal identification number that is required to allow you to use your Android Device to access and use your Cards to make purchases through Google Pay is kept secure in the same way as a cardholder would a banking password or PIN, including but not limited to, by:

- Not disclosing or sharing with anyone;
- Not carrying a record of it with an Android Device or anything liable to be stolen with an Android Device (unless a reasonable effort is made to protect the security of the device);
- Not choosing an easily guessable passcode such as the cardholder's date of birth or a recognisable part of the cardholder's name; and
- Not acting with negligence in failing to protect the security of the passcode.

You must take all steps and prevent any fraud, loss, or theft in respect of your Android Device or any of your Cards in connection with the use of Google Pay.

If biometric identifiers are registered on your Android Device and are used to identify you or be used to grant access to and use your Card for Google Pay, you must not save a third party's biometrics such as fingerprint (biometric information) on the device. In the event a third party's biometrics are saved on the device, whether now or in the future, and such biometric details can be used to grant access to the device to access and use your Card, you understand, acknowledge and agree that you will be taken to have authorised that person to transact on your behalf and the relevant transactions will be charged to your Card, to which you shall be responsible and liable for the same.

If you enroll for biometric verification such as fingerprint identity ("**Touch ID**"), personal identification number or passcode on Google Pay, the collection, storage, enrolment, and access to Google Pay using your biometric information, personal identification number or passcode will be made using the technology on your Android Device. Accordingly, when you

log into Google Pay and choose to be verified using the technology on your Android Device, your fingerprint or any other biometric information, personal identification number, or passcode will be matched and verified against your device's technology. Accordingly, you acknowledge that we have no control over the technology on the Android Device, the availability, capability, verification method, security, and integrity of the Android Device and cannot be held responsible for transactions effected using Google Pay and authorized using any biometric information or personal identification number or passcode. You should therefore assess if the Android Device's manner of verification and risks associated with such use is acceptable to you.

The use of Google Pay is at your discretion. You are not obliged to use Google Pay in connection with any of your Cards. Accordingly, you agree that the access and use of your Card on Google Pay will be considered as authorized by you and you shall be responsible and liable for the same. If you share your passcode with any other person, you are taken to have authorized that person to transact on your account using Google Pay. This means that any Google Pay transaction initiated by that person using the fingerprint or passcode will be authorized by you and the clauses of the Agreement which deal with unauthorized transactions will not apply. If your Android Device is lost or stolen, any biometric information or personal identification number or other passcode is compromised or used or your Card has been used through Google Pay without your permission, you must notify us immediately and if we so require, furnish to us a statutory declaration in such form as we specify and/or a police report and/or any other information we may reasonably require. You are liable for all unauthorized use of your Card in connection with Google Pay until you notify us unless we determine, at our sole discretion that: (i) you have fully complied with these Terms (including, but not limited to the safety precautions) and you notified us without delay, (ii) you assist in the investigations and recovery, and (iii) we are satisfied that such unauthorized transactions are not due to your wilful misconduct and/or gross negligence and that you have not acted fraudulently.

You agree and acknowledge that the transaction history displayed in Google Pay in connection with the use of your Card in Google Pay solely represents our authorization of your Google Pay transaction using that particular Android Device and does not reflect any post-authorization activity, including but not limited to clearing, settlement, foreign currency exchange, refunds, returns or chargebacks.

Accordingly, the purchase amount, currency, and other details for your Google Pay transaction history in connection with the use of your Card in Google Pay may not match the transaction amount that is ultimately cleared, settled, and posted to your Card statement of account. If there is any inconsistency between your Card statement of account and the transaction history displayed in Google Pay, your Card statement of account shall prevail, and you will remain liable to us for the amounts set out on your statements.

Fees and charges

All applicable fees, interests, and charges that apply to your Card pursuant to the Agreement are available and provided on our website and will continue to apply after you have registered your Card with Google Pay. We currently do not impose any additional fees for using your Card through Google Pay but we reserve the right to impose a fee at our sole discretion in the future. You shall be solely responsible for all third-party charges, such as your telecommunications carrier or provider may impose web-enablement, data usage, or text messaging fees and/or other charges associated with your use of Google Pay.

As a condition of using your Card in connection with Google Pay, you acknowledge and consent to us sending notifications and automatically dialed calls or text messages to the Android Device which may or may not be the same device as your mobile phone number on record with us.

Suspension and termination of Google Pay

We have the right to suspend, block, or cancel your ability to use your Card in connection with Google Pay at any time and need not give you any prior notice or reason for doing so, including, modifying or suspending the type of transactions allowed on your Card in connection with Google Pay, change the eligibility of a Card for use with Google Pay, and/or change the Card authentication process.

We also have the right to impose a limit on any daily and/or individual transaction amount(s) charged to your Card through Google Pay. The limit will be at such amount(s) as determined by us and notified to you from time to time.

In the event we have canceled or suspended your Card in accordance with these Terms and/or the terms of the Agreement, you will not be allowed to use it through your Android Device. Please note that this is the case even though you may still see a symbol for the Card on your Android Device.

Authorization to collect and share data

You agree that we may collect, transmit, store, and use technical, location, and login or other information about you and your use of your Card through Google Pay. We may also collect information relating to your Android Device (including app version, device type and model, operating system, and security information such as whether you have obtained root access):

- To ensure your Card properly functions in Google Pay;
- For security purposes and to identify fraud;
- For Card Issuer to better provide assistance to you; and
- To tell you about other products or services that may be of interest to you.

You acknowledge that (i) Google, the provider of Google Pay technology that supports your Card in Google Pay, as well as its subcontractors, agents, and affiliates, and (ii) the applicable payment network branded on your Card (i.e., Visa) as well as subcontractors, agents, and affiliates of such payment networks, will have access to certain details of your transactions made with merchants via use of your Card through Google Pay in and/or for the purposes of (1) performing its obligations hereunder; (2) providing you with relevant transaction data; (3) detecting and addressing fraud; (4) complying with applicable laws and regulations; (5) responding to inquiries made pursuant to court orders or by regulators; (6) managing, making product enhancement to, and/or promoting the use of Google Pay; and (7) creating business and/or technical performance reporting. You acknowledge that the use, storage, and disclosure of any personal information provided by you directly to Google, the applicable payment network branded on your Card (i.e., Visa), or other third parties supporting Google Pay, will be governed by the privacy policy of such party.

Merchant relationships and disclaimers

Merchants may present to you certain discounts, rebates, or other benefits (e.g. free shipping) ("**Offers**") if payment is effected through Google Pay. Such Offers are subject to certain terms and conditions between you and the relevant merchant. We will not be liable for any

loss or damage as a result of any interaction between you and a merchant with respect to such Offers. All matters, including delivery of goods and services, returns, and warranties, are solely between you and the applicable merchants. You acknowledge that we do not endorse or warrant the merchants that are accessible through Google Pay or the Offers that they provide.

Changes to Terms and Conditions
We may amend at any time these Terms, by providing reasonable prior notice to you. We may revise these Terms at any time by updating this posting. You are bound by such revisions and should therefore visit our website to review the current Terms from time to time.

Intellectual Property
All intellectual property rights including all patents, trade secrets, copyrights, trademarks, and moral rights (collectively, "**Intellectual Property Rights**") in Google Pay (including text, graphics, software, photographs and other images, videos, sound, trademarks and logos) are owned either by Google, us, our licensors or third parties. Nothing in these Terms gives you any rights in respect of any intellectual property owned by Google, us, our licensors, or third parties and you acknowledge that you do not acquire any ownership rights by adding your Card to, or using your Card in connection with, Google Pay.

Disclaimers of warranty
Google Pay is provided by Google and without warranty from us. You acknowledge and agree that from time to time, your use of the Card in connection with Google Pay may be delayed, interrupted, or disrupted for an unknown period of time for reasons we cannot control. Neither we nor our affiliates will be liable for any claim arising from or related to the use of your Card through Google Pay due to such delay, interruption, disruption, or similar failure.

You acknowledge that we are not party to the terms and conditions for Google Pay between you and Google and we do not own and are not responsible for Google Pay. We are not providing any warranty for Google Pay. We are not responsible for performance, maintenance, or other support services for Google Pay and shall not be responsible for any other claims, losses, liabilities, damages, costs, or expenses with respect to Google Pay, including, without limitation, any third-party product liability claims, claims that Google Pay fails to conform to any applicable legal or regulatory requirement, claims arising under consumer protection or similar legislation, and claims with respect to intellectual property infringement. Any inquiries or complaints relating to the use of Google Pay, including those pertaining to Intellectual Property Rights, should be directed to Google.

We do not recommend, endorse or make any representation or warranty of any kind regarding the performance or operation of your Android Device. You are responsible for the selection of an Android Device and for all issues relating to the operation, performance and costs associated with such Android Device.

Limitation of liability
To the maximum extent permitted by applicable law, in no event shall we, our processors, suppliers, or licensors (or their respective affiliates, agents, directors, and employees) be liable for any direct, indirect, punitive, incidental, special, consequential, or exemplary damages, including without limitation damages for loss of profits, goodwill, use, data, or

other intangible losses, that result from the use of, inability to use, or unavailability of Google Pay, including your use of Card in connection with Google Pay.

To the maximum extent permitted by applicable law, we, our processors, suppliers, and licensors (and their respective affiliates, agents, directors, and employees) assume no liability or responsibility for any (i) errors, mistakes, or inaccuracies of content; (ii) personal injury or property damage, of any nature whatsoever, resulting from your access to or use of Google Pay, including your use of your card in connection with Google Pay; (iii) any interruption or cessation of transmission to or from Google Pay; (iv) any bugs, viruses, Trojan horses, or the like that may be transmitted to or through Google Pay by any third party; (v) any errors or omissions in any content or for any loss or damage incurred as a result of the use of any content posted, emailed, transmitted, or otherwise made available through Google Pay; and/or (vi) user content or the defamatory, offensive, or illegal conduct of any third party.

Indemnity

You will indemnify, defend, and hold us (and our employees, directors, agents, affiliates and representatives) harmless from and against any and all claims, costs, losses, damages, judgments, tax assessments, penalties, interest, and expenses (including reasonable attorneys' fees) arising out of any claim, action, audit, investigation, inquiry, or other proceeding instituted by a person or entity that arises out of or relates to: (a) any actual or alleged breach of your representations, warranties, or obligations set forth in these Terms, including any violation of our policies; (b) your wrongful or improper use of Google Pay, including wilful misconduct or fraud; (c) your violation of any third-party right, including without limitation any right of privacy, publicity rights or Intellectual Property Rights; (d) your violation of any law, rule or regulation of Hong Kong or any other country; (e) any access or use of Google Pay by any other party with your Touch ID or personal identification number or passcode or other appropriate security code, and (f) any change in law, regulations, guidelines or official directive or circulars which has an effect on the Card or Google Pay, and the same may be debited to your Card and/or shall be paid by you on demand.

Representation and warranty

You represent and warrant to us that: (i) to the extent you identified a name at registration, the name identified by you when you registered your Card to be added to Google Pay is your name; (ii) you are the cardholder of all Cards you add to Google Pay; (iii) you and all transactions initiated by you or using any of the Cards added to Google Pay will comply with all laws, rules, and regulations applicable to you, including any applicable tax laws and regulations; (iv) you have the authority to authorize the receipt of notices, calls and text messages from us at the phone number you provide, (v) you will not use any of your Card through Google Pay for any fraudulent undertaking or in any manner to interfere with the operation of Google Pay; (vi) you will not permit any use of your Card through Google Pay by any third party; and (vii) your use of your Card in connection with Google Pay will comply with these Terms.

Removal of your Card from Google Pay

You shall follow the instructions from Google Pay to remove your Card from Google Pay if you no longer wish to use your Card through Google Pay. You should also ensure that any Card is removed from your Android Device before the disposal of the Android Device. Removal of your Card from Google Pay will not terminate your Card unless you also choose to terminate such in accordance with the terms of the Agreement.

Severability
If any provision or part of a provision of these Terms is illegal, invalid or unenforceable, it will be severed from these Terms and the remaining provisions (or parts of provisions) will continue in full force and effect.

Governing law
The same laws that govern the Agreement shall govern these Terms.

Definitions

In these Terms, all capitalised words or expressions used shall be defined and carry the same meaning as stated in the Definition section of the Terms and Conditions of Payment Cards ("**Agreement**") except for the following words defined below:

"**Android Device**" means a device that supports the Android operating system, which Reap determines, at its sole discretion, is eligible for the registration of Card to be used in Google Pay. Any devices that are modified contrary to the software or hardware guidelines of the manufacturer, including by disabling hardware or software controls (commonly referred to as "jailbreaking"), are not eligible for the registration of Card to be used in Google Pay.

"**Google Pay**" means the mobile payment and digital wallet service created by Google that lets users make payments using certain devices that support the Android operating system and credit cards or debit cards registered on such Android Devices.

"**Card Issuer** ", "**Reap**", "**we**" or "**us**" means Reap Technologies Limited and its subsidiaries.
"**You**" means the Company of the Program Account related to the Card which has been added to the Google Pay digital wallet on any Android Device and, as the context requires, includes any relevant Authorized User.

Last updated: 1st day of March, 2024

Intellectual Property notice (the “IP Notice”)

Intellectual Property Rights

The Websites and any Services and their entire contents, features, and functionality (including but not limited to all information, software, text, displays, images, video and audio, and the design, selection, and arrangement thereof), are owned by us, our licensors or other providers of such material and are protected by copyright, trademark, patent, trade secret and other intellectual property or proprietary rights laws.

These IP Notice permit you to use the Websites and the Services for your personal, non-commercial use only. You must not reproduce, distribute, modify, create derivative works of, publicly display, publicly perform, republish, download, store, or transmit any of the material on our Websites and any Services, except as follows:

- Your computer may temporarily store copies of such materials in RAM incidental to your accessing and viewing those materials.
- You may store files that are automatically cached by your Web browser for display enhancement purposes.
- You may print or download one copy of a reasonable number of pages of the Websites for your own personal, non-commercial use and not for further reproduction, publication, or distribution.
- If we provide desktop, mobile, or other applications for download, you may download a single copy to your computer or mobile device solely for your own personal, non-commercial use, provided you agree to be bound by our end user license agreement for such applications.

You must not:

- Modify copies of any materials from this site.
- Delete or alter any copyright, trademark, or other proprietary rights notices from copies of materials from this site.
- Access or use for any commercial purposes any part of the Website or any services or materials available through the Website and any Services.

If you wish to make any use of materials on the Websites or in any Services other than that set out in this section, please address your request to support@rival.finance.

If you print, copy, modify, download or otherwise use or provide any other person with access to any part of the Websites and any Services in breach of the IP Notice, your right to use the Websites and any Services will cease immediately and you must, at our option, return or destroy any copies of the materials you have made. No right, title, or interest in or to the Websites or any Services or any content on the Website or any Services is transferred to you, and all rights not expressly granted are reserved by us. Any use of the Websites not expressly permitted by these IP Notice and Terms & Conditions (available on our website https://rival.finance/) is a breach of these IP Notice and Terms & Conditions and may violate copyright, trademark, and other laws.

Rival Finance AML/KYC Policy

1. Introduction

The Anti-Money Laundering and Know Your Customer Policy (the "**AML/KYC Policy**") of RIVAL PAYMENTS SERVICES PROVIDER LLC, incorporated in United Arab Emirates with a registered number 1308095 and registered office at Dubai, Business Bay, Burlington Tower, Office 403 **("Rival Finance")** and Choise Services UAB ("**Company**", "**Choise**", "we" or "us") is established to prevent and mitigate possible risks of Choise Services UAB being involved in illegal or illicit activities and to enable Choise Services UAB to meet its legal and regulatory obligations in this area (if any, where applicable). This AML/KYC Policy is subject to changes and updates by Choise from time to time to ensure compliance with any applicable legislation and global AML/KYC practices.

Therefore, Choise Services UAB is regulated and compliant with the laws and regulations to combat money laundering and terrorist financing:

- Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania
- Order of FCIS Director No. V-240 on approval of "Money laundering and suspicious monetary operations or transactions recognition criteria list"
- Order of FCIS Director No. V-129 on the approval of "Recommendations for the information submission forms, submission scheme, and filling of submission forms according to the requirements of the Law on the prevention of money laundering and terrorist financing"
- Order of FCIS Director No. V-5 issued 2020-01-10 on the approval of "Instructions for deposit network operators to prevent money laundering and/or terrorist financing "
- Order of FCIS Director No. V-129 on the approval of "Recommendations for the information submission forms, submission scheme, and filling of submission forms according to the requirements of the Law on the prevention of money laundering and terrorist financing"
- Recommendations for Money Laundering of FATF

2. Definitions

"**Beneficial Owner**" means any natural person or persons who ultimately own or control the User (as defined below) and, or the natural person or persons on whose behalf a transaction or activity is being conducted, and

(a) In the case of a body corporate or a body of persons, the beneficial owner shall consist of any natural person or persons who ultimately own or control that body corporate or body of persons through direct or indirect ownership of twenty-five per centum (25%) plus one (1) or more of the shares or more than twenty-five per centum (25%) of the voting rights or an ownership interest of more than twenty-five per centum (25%) in that body corporate or body of persons, including through bearer shareholdings, or control via other means, other than a company that is listed on a regulated market which is subject to disclosure requirements consistent with European Union law or equivalent international standards which ensure adequate transparency of ownership information:

Provided that a shareholding of twenty-five per centum (25%) plus one (1) share or more, or the holding of an ownership interest or voting rights of more than twenty-five percentum (25%) in the customer shall be an indication of direct

ownership when held directly by a natural person, and of indirect ownership when held by one or more bodies corporate or body of persons or through a trust or a similar legal arrangement, or a combination thereof:

Provided further that if, after having exhausted all possible means and provided there are no grounds of suspicion, no beneficial owner in terms of this paragraph has been identified, subject persons shall consider the natural person or persons who hold the position of senior managing official or officials to be the beneficial owners, and shall keep a record of the actions taken to identify the beneficial owner in terms of this paragraph.

(b) In the case of trusts, the beneficial owner shall consist of

i. the settlor;

ii. the trustee or trustees;

iii. the protector, where applicable;

iv. the beneficiaries or the class of beneficiaries as may be applicable; and

v. any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

(c) In the case of legal entities such as foundations and legal arrangements similar to trusts, the beneficial owner shall consist of the natural person or persons holding equivalent or similar positions to those referred to in paragraph (b).

"**High-Risk Jurisdiction**" means the jurisdictions designated by Choise as high risk jurisdiction in respect of any Sale or Service from time to time.

"**Politically Exposed Person**" means a natural person who is or has been entrusted with prominent public functions, other than middle-ranking or more junior officials. For this definition, the term "natural person who is or has been entrusted with prominent public functions" includes the following:

(a) Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;

(b) Members of Parliament or similar legislative bodies;

(c) Members of the governing bodies of political parties;

(d) Members of superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(e) Members of courts of auditors or the boards of central banks;

(f) Ambassadors, charges d'affaires, consuls, and high ranking officers in the armed forces;

(g) Members of the administrative, management, or supervisory boards of State-owned enterprises;

(h) Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) within an institution of the European Union or any other international body;

Furthermore, a Politically Exposed Person includes family members or persons known to be close associates of any individual identified in (a) – (h) above.

The term “family members” includes:

- the spouse, or a person considered to be equivalent to a spouse;
- the children and their spouses, or persons considered to be equivalent to a spouse; and
- the parents.

“Persons known to be close associates” means:

- a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relations, with that politically exposed person; or
- a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that politically exposed person.

“**Prohibited Jurisdiction**” means the jurisdictions designated by Choise as prohibited jurisdiction in respect of the Sale or Service from time to time.

“**Sanctioned Jurisdiction**” means any country or territory to the extent that such country or territory is the subject of any sanction issued by the United Nations, United States, and/or the European Union.

“**Sanctioned Person**” means any individual or entity (a) identified on a sanctions list issued by the United Nations, United States, and/or the European Union; (b) organized, domiciled, or resident in a Sanctioned Jurisdiction; or (c) otherwise the subject or target of any sanctions, including because of ownership or control by one or more individuals or entities described in clauses (a) or (b).

“**Service**” means any other services provided by Choise to the Users from time to time, including, without limitation, its payment and cryptocurrency exchange services, wallet services, Instachange.com services, and any other services or functionalities, past, present, or future.

“**Transaction**” means any transaction with any assets that is conducted by a user through any of Choise’s websites, applications, client accounts, cryptocurrency wallets, Services, or functionalities, and the word “transact” shall be interpreted accordingly.

“**User**” means a person using Choise’s Services.

3. Initial and ongoing screening

a) Choise will (and will always reserve a right to) screen a User before enabling any Transaction with such User and will continue to screen such User on an ongoing basis, to ensure that such User is not a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction (through third parties, including Crypterium AS).

b) Choise will screen a User before providing any Service to such User and will continue to screen such User on an ongoing basis, to ensure that such User is not a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction. If a User is a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction, Choise will refuse to provide Services to such User or discontinue the provision of Services.

In carrying out this screening Choise shall ensure to adopt software to enable comprehensive screening to be carried out and which captures all sanctions that Choise is bound to follow.

4. KYC/AML identification procedures

Choise adopts a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, Choise can ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks.

Before enabling or entering into a Transaction with or for or on behalf of a User or providing any Service to a User, Choise will, if so required by applicable law or if it is otherwise deemed necessary or expedient:

a) identify the User and verify the User's identity based on documents, data, or other information based on a reliable and independent source (through third parties, including Crypterium AS);

b) If there is a Beneficial Owner concerning the User, identify the beneficial owner and take reasonable measures to verify the beneficial owner's identity;

c) obtain information on the purpose and intended nature of the business relationship with the User, unless the purpose and intended nature are stipulated in the relevant documentation between Choise and the User. As part of this process, Choise shall obtain, amongst other matters, information on the source of funds and source of wealth of the User; and

d) if a person purports to act on behalf of the User, (i) identify the person and take reasonable measures to verify the person's identity based on documents, data or information based on a reliable and independent source; and (ii) verify the person's authority to act on behalf of the User.

To identify a User who is an individual, Choise will collect information from the User, including but not limited to, his full name, date of birth, place of birth, nationality, place of residence, email address, and the identity document type. Choise will verify the identity of the User with documents such as his national ID, passport, and/or driver's license and utility bill (through third parties, including Crypterium AS).

To identify a User who is a legal entity, Choise will collect information from the User, including but not limited to, its full legal name, registration number, date of incorporation/registration, country of incorporation/registration, and lists of directors (as applicable to the entity). Choise will verify the User with documents such as Memorandum and Articles of Association (or equivalent), additional beneficial ownership information and documents, and a detailed corporate chart (as applicable

to the entity).

If the User is not physically present for identification purposes, Choise may adopt more stringent standards to verify the identity of the User.

Documents in languages other than English must be translated into English; the translation must be notarized and sent along with a copy of the original document with a clear photograph.

For additional verification, We duly perform User verification using the following method - Skype, Zoom conference calls, or other types of communication regarding the «Face to Face» procedure of verification.

5. Ongoing monitoring of Users

Choise reserves the right to continuously monitor, on a risk-sensitive basis, the business relationship with a User (as applicable) by:

a) reviewing from time to time documents, data, and information that have been obtained by Choise to ensure that such documents, data, and information are up to date (through third parties, including Crypterium AS);

b) conducting appropriate scrutiny of Transactions and activities carried out by Users to ensure that they are consistent with Choise's knowledge of the User's business and risk profile, and to ensure that such Transactions and activities are in line with Choise's knowledge of the User's or User's source of funds and source of wealth; and

c) identifying transactions that are unusually large in amount or of an unusual pattern and have no apparent economic or lawful purpose.

For the avoidance of doubt, Choise may undertake ongoing monitoring of Users to ensure that any Transactions equal to or above € 500 (or its equivalent in any other currency) shall be subject to enhanced due diligence concerning the source of funds and source of wealth of the User.

To continuously monitor the business relationship with a User (as applicable), Choise may carry out a file review to ensure that information held about the User is up-to-date and that identification documents held are still valid. In addition, on a more frequent basis, Choise may also monitor transactional activity to identify any red flags or 'out of the norm' activity.

As part of the second line of defense, the Money Laundering Reporting Officer will carry out checks to ensure that regular and effective ongoing monitoring is being effected and that irregular or suspicious activities are effectively escalated.

AML online check services that are based on the AML Global Watchlist (global AML risk data sources including sanction lists (such as OFAC, UN, HMT, EU, DFAT, and many more), law enforcement lists (Interpol, country-specific government and state agencies, and police forces), and international governing regulatory bodies (financial and securities commissions).

6. Sanctioned Jurisdictions, Prohibited Jurisdictions, and High Risk Jurisdictions

Choise will establish and maintain the following lists of jurisdictions (i) Sanctioned Jurisdictions (ii) Prohibited Jurisdictions and (iii) High-Risk Jurisdictions. In determining the list of Sanctioned Jurisdictions, Prohibited Jurisdictions, and High-Risk Jurisdictions, Choise shall take into account the lists issued by the Financial Action Task Force and by other organizations issuing guidelines and lists relating to the adequacy of legislative measures adopted by jurisdictions concerning money laundering, funding of terrorism and transparency.

Users who are (i) residents or domiciled in, or (ii) have their source of wealth or source of funds linked to a Sanctioned Jurisdiction and/or a Prohibited Jurisdiction shall not be accepted as clients of Choise.

Users who are (i) residents or domiciled in, or (ii) have their source of wealth or source of funds linked to High-Risk Jurisdictions shall be subject to additional checks and measures by Choise.

7. High risk situations

In certain circumstances, the risk may be higher and Choise will need to take additional checks. These include, for example, situations where the User is from a High-Risk Jurisdiction, where the User is a Politically Exposed Person, or where the User's or User's behavior and activities raise other red flags.

In a high-risk situation, Choise will:

a) where a business relationship has not yet been established, obtain approval from senior management to establish the business relationship and take reasonable measures to verify the User's or beneficial owner's source of wealth and source of funds that will be involved in the business relationship; and

b) where a business relationship has been established, obtain approval from senior management to continue the business relationship, take reasonable measures to verify the beneficial owner's identity, and take reasonable measures to verify the User's or beneficial owner's source of wealth and source of funds that will be involved in the business relationship.

8. **Record-keeping**

Choise will keep (a) transaction records, for ten (10) years beginning on the date on which a transaction is completed, or for such other minimal period as may be required by applicable law; and (b) other information collected by Choise for AML/KYC purposes, throughout the continuance of the business relationship with the User and for ten (10) years beginning on the date on which the business relationship with the User ends, or for such other minimal period as may be required by applicable law.

9. Money Laundering Reporting Officer

The Money Laundering Reporting Officer shall be the person, duly authorized by Choise, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Money Laundering Reporting Officer's responsibility to supervise all aspects of Choise's anti-money laundering and counter-terrorist financing. Once such an officer is appointed, all our employees will report any suspicious behavior or activities to the Money Laundering Reporting Officer.

10. Reporting

Where Choise suspects that a User is involved in any money laundering, terrorist financing, or other illegal activities, it will report any relevant knowledge or suspicion to governmental and regulatory authorities. Choise shall not notify any Users of any such suspicious transaction report. Rather, if Choise and its employees notify such Users, they may be held liable for tipping off. This is a criminal offense punishable by a fine and/or imprisonment.

Last updated: 26th April 2024

Privacy Policy

Welcome to the Privacy Policy (the "**Policy**").

This Website and Mobile application are owned by the company RIVAL PAYMENTS SERVICES PROVIDER LLC, incorporated in United Arab Emirates with a registered number 1308095 and registered office at Dubai, Business Bay, Burlington Tower, Office 403 **("Rival Finance")**.

Choise Services UAB, a legal entity duly registered in Lithuania with No. 305964183 with a registered office at Vilnius, Eišiškių Sodų 18-oji g. 11. (the "**Choise**") and Charism LLC, is a limited liability company created and existing under the laws of Saint Vincent and Grenadines, with company number 1999 LLC 2022, registered office at Suite 336, Beachmont Business Centre, Kingstown (the "**Associated Company**").

As a high-level summary, we are an evolving cryptocurrency-focused financial institution providing various cryptocurrency-related financial services (the "**Services**"). We provide all this employing the website https://rival.finance/ (the "**Website**") and the related mobile application and crypto-platforms that we may operate from time to time (each of which, is a "**Platform**") and which may be accessible via the Website or otherwise.

Accordingly, the purpose of this Policy is to set out the basis on which we will process your data when you:

1. visit and use a Website and/or Platform, regardless of where you visit or use them from;

2. apply for and register a customer account with us (your "**Account**");

3. apply for, receive, pay, and/or use any of our Services.

This also includes any data that you may provide to us for our events, newsletters, and other marketing items.

This Policy informs you about the items of Personal data that we may collect about you and how we will handle it, and in turn, also tells you about

(i) our obligations to process your data responsibly,

(ii) your data protection rights as a data subject, and (iii) how the law protects you. It should be read in conjunction with our Cookie Policy.

Please read the following information carefully to understand our practices regarding your data.

1. Important information and who we are

General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) regulations shall be implemented for EU users (the "**Regulation**" or the "**GDPR**").

This Policy aims to ensure that you are fully informed on how we will collect and process your Personal data in the circumstances and scenarios outlined in the **'Introduction'** (namely, through your token subscriptions and purchases, your use of the Website, and any of the related Services).

The Websites, the Platform, and the Services are not intended or in any way made available for minors, and we do not knowingly collect data relating to minors.

You must read this Policy together with any other privacy or fair processing notice we may provide on specific occasions when we are collecting or processing Personal data about you so that you are fully aware of how and why we are using your data. This Policy supplements the other notices and is not intended to override them.

The opening and registration of a customer account will give rise to the existence of a contractual relationship with us, as regulated by our Terms of Use, and all matters between you and us relating to Services will be deemed to fall within the subject matter of that same contractual relationship. Furthermore, the existence of this contract between you and us will also serve as the legal basis for a number of our processing activities involving your Personal data, as detailed below.

Controllers

RIVAL PAYMENTS SERVICES PROVIDER LLC (as defined) above is the controller and is responsible for your Personal data. There may be other controllers of your Personal data, such as, for example, electronic identification verification service providers, Associated companies, or other service providers engaged by us for purposes of processing and storing your Personal data. They will be so-called "joint controllers" of your Personal data and as such, will share responsibility for such control with us.

Presently, we use the services of the following service providers:

Ondato: https://www.ondato.com for KYC/AML verification;

Vero: https://www.getvero.com or handling e-mail lists and campaigns; and

Walletto: https://walletto.eu for card-issuing services;

In the course of providing our services to you, we may transfer your personal data to certain third-party legal entities for the purpose of issuing bank cards, facilitating financial transactions, and other related services. Specifically, your personal data will be shared with Reap Technologies Limited and Layer 2 Financial Inc.

These entities have been carefully selected to ensure that your personal data is processed in a manner consistent with our commitment to safeguarding your privacy. Reap Technologies Limited and Layer 2 Financial Inc. will process your personal data in accordance with their established privacy policies, which outline their practices regarding the collection, use, processing, and protection of personal data.

To understand how your personal data will be handled by these entities, you are encouraged to review their privacy policies:

- Reap Technologies Limited: https://reap.global/privacy-policy

By agreeing to this Privacy Policy, you consent to the transfer of your personal data to Reap Technologies Limited and for the purposes outlined above. We ensure that such transfers

are conducted in compliance with applicable data protection laws and regulations and that adequate safeguards are in place to protect your personal data.

Please familiarize yourself with these providers and their privacy and liability policies. If you find any of these may not work for you, please do not access any of the Websites and do not use any of our Services.

As a general rule, we always seek to minimize the amount of your Personal data that we collect and store.

Contact details

Full name of legal entity: RIVAL PAYMENTS SERVICES PROVIDER LLC

Email address: legal@rival.finance

Please use the words 'Data Protection Matter' in the subject line.

Changes to the Policy and your duty to inform us of changes

It is imperative that the Personal data we hold about you is accurate and current at all times. Otherwise, this will impair our ability to process your token purchases and/or our ability to provide you with the Services that you may request from us (amongst other salient issues).

Please keep us informed if any of your Personal data changes during your relationship with us.

Third-party links

Our Website may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy notice or policies. We strongly encourage you to read the privacy notice of every website you visit, particularly when leaving our Website.

2. Glossary

Set out below are key definitions of certain data protection terms that appear in this Policy.

"**Consent Form**" refers to separate documents that we might from time to time provide you where we ask for your explicit consent for any processing that is not for purposes set out in this Policy.

"**Data subjects**" means living individuals (i.e. **natural persons**) about whom we collect and process Personal data.

"**Data controller**" or "**controller**" means any entity or individual who determines the purposes for which, and how, any Personal data is processed.

"**Data processor**" or "**processor**" means any entity or individual that processes data on our behalf and on our instructions (we being the data controller).

"**Personal data**" means data relating to a living individual (i.e. **natural person**) who can be identified from the data (information) we hold or possess. This includes but is not limited to, your name and surname (including maiden name where applicable), address, date of birth, nationality, gender, civil status, tax status, identity card number & passport number, contact details (including mobile and home phone number and personal email address), photographic image, bank account details, emergency contact information as well as online identifiers. The

term “**personal information**”, where and when used in this Policy, shall have taken the same meaning as Personal data.

“**Processing**” means any activity that involves the use of Personal data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal data to third parties.

“**Sensitive Personal data**”, “**sensitive data**” or “**special categories of Personal data**” includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offense committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. This type of sensitive data can only be processed under strict conditions.

Note that Personal data does not include information relating to a legal person (such as for example, a company). Therefore, information such as a company name, its company number, registered address, and VAT number, does not amount to Personal data in terms of both the Act and the GDPR. Naturally, we will still treat any such information confidentially and securely.

3. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (**anonymous data**).

We may collect, use, store, share, and disclose different kinds of Personal data about you which (**for purely indicative purposes**) we have grouped as follows. For the avoidance of doubt, categories marked in blue do not apply to non-customers (i.e. individuals who do not hold a registered customer account with us).

- **Identity Data** includes your first name, maiden name (where applicable), last name, username or similar identifier, marital status, title, nationality, date of birth, gender, identity card, and/or passport number.

- **Contact Data** includes address, billing address, email address, and contact number (telephone and/or mobile).

- **AML and KYC Data** includes the following due diligence documentation and information on you:

(i) copy of your national identity document, passport, and/or driver’s license, (ii) proof of residence (for example, a recently issued utility bill), (iii) a ‘selfie’ (for identity verification), (iv) KYC database checks, (v) fraud database checks and (vi) any documentation or information which we may be from time to time:

1. required to collect to ensure compliance with any applicable legislation (including applicable foreign laws) and global AML/KYC practices; and/or

2. otherwise mandated to collect by any competent authority, including, as applicable, any other documentation or information which may be mandated on us from time to time by applicable law and by any other competent authority or related legislation (including overseas authorities and applicable foreign laws).

- **Enhanced KYC Data** applies with respect to payments that exceed a set threshold and includes, at a minimum, the following enhanced customer due diligence documentation and information: source of funds and source of wealth.

- **Financial Data** includes your wallet and private key details.

- **Transaction Data** includes details about:
    1. your subscriptions, purchases, and transactional activity;
    2. your transactional history on the Platform;
    3. your use of the Services (including your service requests);
    4. the payments made to and from you.
- **Portfolio Data** includes details about the tokens credited to your account.
- **Usage Data** includes details about how you use our Platform and the Websites.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type, and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices which you (whether a client or otherwise) use to access and browse the Websites.
- **Website Visit Data** includes the full Uniform Resource Locators (URL), clickstream to, through, and from the Website (including date and time), products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us or our third parties and your communication preferences. This may include information on whether you have subscribed or unsubscribed from any of our mailing lists, attended any of our events, or accepted any of our invitations.

We will also collect, use, and process any other information that you voluntarily choose to provide or disclose to us where relevant for processing your token requests and/or providing you with your requested Services. Any such information that we receive from you would fall under the '**Transaction Data**' category.

We also collect, use, and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data may be derived from your Personal data but is not considered Personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Website Visit Data to calculate the percentage of users accessing a specific feature of the Website. However, if we combine or connect Aggregated Data with your Personal data so that it can directly or indirectly identify you, we treat the combined data as Personal data which will be used following this Policy.

If you fail to provide Personal data

Where we need to collect Personal data about you:

- by law, or
- under the terms of, or in connection with, the contract that we have with you (as discussed above); or
- as part of our legitimate (business) interests to verify the identity of our applicants and customers, mitigate against risks (such as potential or suspected fraud), and, in particular, assess and take a decision on whether we want to enter into a customer relationship with you (as subject to our customer acceptance criteria and policies),

and you either fail to provide that data when requested, or else provide incomplete or insufficient data, we may not be able to perform or conclude the contract that we have or are otherwise trying to enter into with you (namely regarding your account opening, token subscriptions and purchases, and provision of the Services).

In certain cases, particularly where it relates to KYC due diligence data (both standard and enhanced), we may even need to exercise our prerogative to terminate our contract with you following the terms thereof, or else, if still at the application stage, we may have to decline to enter into a customer relationship with you.

We will however notify you if this is the case at the time.

Special categories of Personal data

We do not knowingly collect Special Categories of Personal data (or Sensitive Personal data) about you. Should we receive sensitive Personal data about you, we will only process that data when there is a legitimate basis to do so and, in all circumstances, in accordance with our obligations at law and under the appropriate safeguards.

As set out below in **Section 5**, we collect and process **AML** and **KYC Data** and, if applicable, **Enhanced KYC Data** in order to (i) conduct our AML and KYC checks, and other due diligence checks, on you, (ii) verify your identity or claimed identity and, in those instance of enhanced due diligence, your source of funds and source of wealth, (iii) take an informed decision on whether we want to enter into a customer relationship with you, and, if positive, to conduct initial and ongoing screening and monitoring and (iv) to comply with any legal or regulatory obligation that we may have and/or any Court, regulatory or enforcement order that may be issued upon us.

4. How is your Personal data collected?

We generally use different methods to collect data from and about you including through:

Account Registration. We will ask you to provide us with your Identity, Contact AML, and Risk Data when you apply to open a customer account with us. You provide this information, which will then be collected and processed when you fill in and submit your account application form (together with other related forms) and complete the required application steps.

Direct Interactions. You may give us your Identity, Contact AML and Risk Data, Enhanced KYC Data, and Marketing and Communications Data by filling in our forms (such as our 'Contact Form') or by corresponding with us by post, phone, email, or otherwise. This includes Personal data you provide when you:

- contact us in the context of opening and registering a customer account;
- apply to open a customer account;
- subscribe to, purchase, and/or use our Services;
- discuss with us the particular Services that you require;
- request and receive our Services;
- contact us with complaints or queries;
- complete an inquiry form;
- contact us for further information about our products and services;
- submit the AML and KYC Data and/or Enhanced KYC Data that we request;
- request marketing to be sent to you;
- express interest and/or attend any of our seminars or other hosted events;
- participate in a survey or our webinars;
- subscribe to our newsletters;
- give us some feedback.

Through our provision of the Services. This may encompass all of the data categories listed in Clause 3 (namely, Identity, Contact, AML and Risk Data, Enhanced KYC Data, and Transaction Data).

Automated technologies or interactions. When you interact with our Website, we may automatically collect Technical and Usage Data about your equipment, browsing actions,

and patterns. We may collect this Personal data by using cookies, server logs, and other similar technologies.

Please see our Cookie Policy for further details.

Third parties or publicly available sources. We may receive Personal data about you from various third parties and public sources as set out below:

Technical Data from the following parties:

(a) analytics providers;

(b) advertising networks; and

(c) search information providers.

Identity, Contact, AML, and Risk Data and Enhanced KYC Data from publicly available sources such as public court documents, the RoC, and the company houses and registers of other jurisdictions, and from electronic data searches, online KYC search tools (which may be subscription or license-based), anti-fraud databases and other third party databases, sanctions lists, outsourced third-party KYC providers and from general searches carried out via online search engines (e.g. Google).

We may also receive customer due diligence reports about our applicants from our outsourced third-party KYC provider. These reports may encompass identity checks, document integrity checks, checks against global sanctions lists, and related screening and monitoring measures. In such cases, this third-party provider will conduct the requested customer due diligence checks **autonomously** and will generally amount to a controller of the Personal data that it collects in connection with those checks. It also has its data policies and practices, which will be duly notified and communicated to the applicant.

5. How we use your Personal data

We will only use your Personal data when the law allows us to. Most commonly, we will use your Personal data in the following circumstances:

Where you wish to enter into a customer relationship with us.

Where we need to perform the contract we have or which are about to enter into with you as a customer (including in respect of your token purchases and subscriptions, and use of the Services).

Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

Where we need to comply with a legal or regulatory obligation.

You have the right to withdraw consent to such marketing at any time by contacting us, as indicated above under '**Contact Details**'.

6. Purposes for which we will use your Personal data

We have set out below, in a table format, a description of all the ways we plan to use your Personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your Personal data according to more than one lawful ground or basis, depending on the specific purpose for which we are using your data. Please contact us at legal@rival.finance if you need details about the specific lawful basis we are relying on to process your Personal data where more than one lawful basis has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
(a) To conduct customer due diligence measures on you (following your application to enter into a customer relationship with us). (b) To determine whether we want to enter into a customer relationship with you and, if positive, to register your customer account and onboard you as a customer.	(a) Identity; (b) Contact; (c) AML and KYC.	(a) Performance of a contract with you or to take steps at your request before entering into such a contract. (b) Necessary for our legitimate interests (to verify your identity, conduct initial screening and monitoring (sanctions lists, fraud databases, and other KYC checks), determine whether you present any risks as a prospective customer, and ultimately enable us to take an informed decision on whether we want to enter into a customer relationship with you).
(a) To establish and verify your identity. (b) To fulfill our other internal KYC policies and requirements.	(a) Identity; (b) Contact; (c) AML and KYC; (d) Enhanced KYC Data (for payments over a certain threshold); and (e) Transaction.	Necessary for our legitimate interests (for risk assessment purposes, to prevent and mitigate against fraud, to safeguard the reputation of our business).
(a) To enable your use of the Platform, process your token subscriptions, purchases, and trading activity, and provide you with the Services that you have requested from us. (b) To keep your account portfolio accurate and updated. (c) Manage transactions and generate transaction reports and records.	(a) Identity; (b) Contact; (c) Financial; (d) Transaction; and (e) Portfolio.	(a) Performance of a contract with you. (b) Necessary to comply with our contractual obligations. (c) Necessary to comply with a legal obligation.

For tax and accounting purposes (e.g. reporting to tax authorities, and accounting and reporting requirements).	(a) Identity; (b) Contact; (c) Financial; and (d) Transaction.	Necessary to comply with a legal obligation.

(a) For billing and invoice purposes; (b) To collect and recover money which is owed to us (debt recovery); (c) Internal record keeping (including files).	(a) Identity; (b) Contact; (c) Financial; (d) Transaction; and (e) Portfolio.	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation. (c) Necessary for our legitimate interests (to recover debts due to us, to keep track of your token subscriptions and purchases and the provision of the Services to you (including any developments that took place), and to then be able to review such information should an issue arise).
To manage our customer relationship with you, which may include to: (a) notify you about changes to our terms of service or privacy notices; (b) set up, manage and administer your customer account on the Website; (c) distribute and account your funds; (d) deal with your enquiries, requests, complaints or reported issues; (e) contact you in the course of providing the requested services; (f) ask you to participate in a survey; (g) request feedback from you; (h) advise you of industry	(a) Identity; (b) Contact; (c) Financial; (d) Transaction; (e) Usage; (f) Portfolio; and (g) Marketing and Communications.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests (for customer relationship handling and management, to study business growth and possible trends regarding our products and service areas, to enable a review and assessment of our products and service provision, to develop and grow our business).

and legislative updates, (i) inform you about our events and seminars (including webinars); (j) provide you with information about our products and services; (k) provide you with any other information or materials which you have requested from us.		

(a) To detect, prevent, and/or report fraud or any other potentially illegal or prohibited activity that comes to our attention. (b) To assist and cooperate in any criminal or regulatory investigations against you, as may be required of us. (c) To enforce our service terms. (d) To protect the rights and property of ourselves and others.	(a) Identity; (b) Contact; (c) AML and KYC; (d) Enhanced KYC; (e) Data; (f) Financial; (g) Transaction; and (h) Payment.	(a) Necessary to comply with a legal obligation. (b) Necessary for our legitimate interests (including, to protect the reputation of our business).
To administer and protect our business, the Website, and our Platform (including troubleshooting, data analysis, testing, system maintenance, support, reporting, and hosting of data).	(a) Identity; (b) Contact; (c) Usage; (d) Technical; and (e) Website Visit.	(a) Necessary for our legitimate interests (for running and administering our business (including IT support), systems administration, network security, preventing fraud and to maintain the confidentiality of communications, and in the context of a business reorganization or group restructuring exercise). (b) Necessary to comply with a legal obligation.

(a) To carry out market research campaigns; (b) To market our products and services to you by email or other means if you have subscribed to one of our mailing lists (where you are not a customer); (c) To deliver relevant Website content and advertisements to you, and measure or understand the effectiveness of the advertising that we serve to you.	(a) Identity; (b) Contact; (c) Technical; (d) Usage; (e) Website Visit; and (f) Marketing and Communications.	(a) Necessary for our legitimate interests (to develop our products and services and grow our business, to define our customers, to keep our products, services, and the Website updated and relevant, and to inform our marketing strategy). (b) Based on your consent, in the absence of a customer relationship.

To permit us to pursue available remedies or limit any damages which we may sustain.	(a) Identity; (b) Contact; (c) AML and KYC; (d) Enhanced KYC; (e) Data; (f) Financial; (g) Transaction; (h) Portfolio; and (i) Marketing and Communications.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests.

"Legitimate Interest" means our interest to conduct and manage our business affairs appropriately and responsibly, to protect the reputation of our business, and to provide our customers with the best possible service and the users of the Websites with a secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before your Personal data is processed for our legitimate interests. We do not use your Personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us at the following email address: legal@rival.finance

"Performance of Contract" means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract. This includes our Terms of Service or other applicable terms of business.

"Comply with a legal obligation" means processing your Personal data where it is necessary for compliance with a legal or regulatory obligation to which we are subject.

7. Marketing

We strive to provide you with choices regarding certain Personal data uses, particularly around advertising and marketing. Through your Identity, Contact, Usage, Technical, and Website Visit Data, we can form a view of what we think you may want or need. This is how we then decide which of our products and/or services may be relevant or of interest to you (our **marketing communications**).

You may **receive marketing communications** from us (which may consist of newsletters, industry and legislative updates, mailshots, publications, and/or information about our events, seminars, and webinars) where:

- you have entered into an ongoing commercial or contractual relationship with us; and
- provided you have not opted out of receiving marketing from us (see **Your right to object** below).

Where the above does not apply to you, we will only send you our marketing communications if you have expressly consented to receive them from us.

Third-Party Marketing

We will get your express opt-in consent before we share your Personal data with any third parties (including our affiliated entities) for marketing purposes.

Opting out

You can ask us to stop sending you marketing communications (unsubscribe) at any time by following the opt-out (unsubscribe) links on any marketing communication sent to you.

Cookies

You can set your browser to refuse all or some browser cookies or to alert you when the Website sets or accesses cookies. If you disable or refuse cookies, please note that some parts of the Website may become inaccessible or not function properly.

Change of purpose

We will only use your Personal data for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose, or we are obliged to process your data by applicable laws or court / enforceable orders.

If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at legal@rival.finance

If we need to use your Personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your Personal data without the need to obtain your consent, in compliance with the above rules, where this is required or permitted by law.

8. Disclosures of your Personal data

We may have to grant access to, disclose, or share your Personal data with the parties set out below (which may be in or outside your jurisdiction) for the purposes set out in the table in **Clause 6** above

Third-party service providers, including platform integration and infrastructure hosting providers (to store data), KYC providers and identity and customer verification service providers (to facilitate the set-up and opening of your account and from whom we may receive customer due diligence reports on you), payment services and payment gateways (to process

payments), and token accounting services (to verify, monitor and secure token subscriptions, purchases and trading activity).

Our affiliated entity, such as partner firms involved in the provision of certain Services.

Affiliated group entities. We share information with these entities to

a) help, detect, and prevent potentially illegal acts and violations of our policies;

b) allow you to use the products and services they provide that are supplied in connection with, or using our products and services; and

c) guide decisions about our products, services and communications.

Suppliers and external agencies that we engage to process information on our or your behalf, including to provide you with the information and/or materials that you may have requested.

Professional advisers such as consultants, bankers, professional indemnity insurers, brokers, and auditors.

Law enforcement agencies, public authorities, and judicial bodies (local and overseas).

Other organizations where the exchange of information is for the purpose of fraud protection or credit risk reduction.

Debt recovery agencies assist us with the recovery of debts owed to us.

Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets (**successors in title**). Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your data in the same way as set out in this Policy.

We require all affiliated entities and third-party service providers to respect the security of your Personal data and to treat it following the law. We do not allow them to use your Personal data for their own purposes and only permit them to process your Personal data for specified purposes and following our documented instructions. Our service providers currently store your Personal data in Germany. We will update this Privacy Policy if their data storage location changes.

6. International transfers

We do not generally transfer your Personal data outside the European Economic Area ("**EEA**") except

as may be necessary to: (i) process your transactions, subscriptions, purchases, and/or trading activity, (ii) provide the requested services, (iii) fulfill our contractual obligations to you, (iv) exercise and enforce our contractual rights and terms of services, (v) comply with our legal and/or regulatory obligations or (vi) assert, file or exercise a legal claim.

Where we do need to transfer your Personal data to outside the EEA (whether for these stated purposes or any other purpose listed in **Clause 5** above), we will ensure a similar degree of protection is afforded to that Personal data by ensuring at least one of the following safeguards applies or is otherwise implemented:

- We will only transfer your Personal data to countries that have been deemed to provide an adequate level of protection for Personal data by the European Commission.

- In the absence of an adequacy decision, we will use specific contracts approved by the European Commission which give Personal data the same protection it has in Europe.

- Where we use providers based in the U.S., we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to Personal data shared between Europe and the US.

Please contact us at legal@rival.finance you want further information on the specific mechanism used by us when transferring your Personal data out of the EEA.

7. Data security

We have put in place appropriate security measures to prevent your Personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed (i.e. to safeguard its integrity and confidentiality). We also regularly review and, where practicable, improve upon these security measures.

We also limit access to your Personal data to strictly those employees, agents, contractors, and third parties that have a professional 'need-to-know'. They will only process your Personal data on our instructions and they are subject to a duty of confidentiality. All our employees and agents have received appropriate training on data protection.

We have put in place procedures to deal with any suspected Personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Data retention

Please note that we consider our relationship with customers to be an ongoing and continuous customer relationship, until such time that either we or the customer terminates it in accordance with our Terms of Use.

We will only retain your Personal data for as long as necessary to fulfill the purposes for which we collected it (see **Clause 6** above) and, **thereafter**:

for the purpose of satisfying any legal, accounting, tax, anti-money laundering, and regulatory obligations or reporting requirements to which we may be subject (including as an issuer of a virtual financial asset in terms of applicable Lithuanian law); and/or

to the extent that we may also need to retain your Personal data to be able to assert, exercise or defend possible future legal claims against you or that otherwise involve you.

By and large, our retention of your Personal data shall not exceed the period of **six (6) years** from the termination of your customer relationship with us (which would typically arise from the closure or termination of your customer account). This retention period enables us to make use of your Personal data for any applicable AML retention and reporting obligations and for the filing, exercise, or defense of possible future legal claims (taking into account applicable prescriptive periods and statutes of limitation). In certain cases, we may need to retain your Personal data for a period of up to **ten (10) years** in order to comply with applicable accounting and tax laws (this will primarily consist of your Transaction Data). There may also be instances where the need to retain Personal Data for longer periods, as dictated by the nature of the products and services provided.

In some circumstances, you can ask us to delete your data. See **Request erasure** below for further information.

Kindly contact us at legal@rival.finance **for further details about the retention periods that we apply.**

Data Minimization

To the extent possible, we may anonymize the data that we hold about you when it is no longer necessary to identify you from the data that we hold about you. In some circumstances, we may even pseudonymize your Personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

9. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your Personal data. Please click on the links below to find out more about these rights:

Request access to your Personal data.

*Request correction (**rectification**) of your Personal data.*

Request the erasure of your Personal data.

Object to processing of your Personal data.

Request restriction of processing your Personal data.

Request transfer of your Personal data.

Right to withdraw consent.

If you wish to exercise any of the rights set out above, please contact us at legal@rival.finance

No fee is usually charged

You will not have to pay a fee to access your Personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may simply refuse to comply with your request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal data (or to exercise any of your other rights). This is a security measure to ensure that Personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within a period of one month from the date of receiving your request. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

You have the right to

(i) **Request access** to your Personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the Personal data we hold about you

and to check that we are lawfully processing it.

You may send an email to legal@rival.finance requesting information on the Personal data that we process. You shall receive one copy free of charge via email of the Personal data that is undergoing processing. Any further copies of the information processed shall incur a charge of €10.00.

(ii) **Right to information** when collecting and processing Personal data about you from publicly accessible or third-party sources. When this take place, we will inform you, within a reasonable and practicable timeframe, about the third party or publicly accessible source from whom we have collected your Personal data.

(iii) **Request correction or rectification** of the Personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected and/or updated, though we may need to verify the accuracy of the new data you provide to us. As mentioned, it is in your interest to keep us informed of any changes or updates to your Personal data that may occur during the course of your relationship with us.

(iv) **Request erasure** of your Personal data. This enables you to ask us to delete or remove Personal data where:

- there is no good reason for us to continue to process it;
- you have successfully exercised your right to object to processing (see below);
- we may have processed your information unlawfully; or
- we are required to erase your Personal data to comply with local law.

Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. These may include instances where the retention of your Personal data is necessary to:

- comply with a legal or regulatory obligation to which we are subject; or
- establish, exercise, or defend a legal claim.

(v) **Object to processing** of your Personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your Personal data for direct marketing purposes (as under the '**Marketing'** in **Section 5** above).

In some cases, we may demonstrate that we have compelling legitimate grounds to process your personal information that override your rights and freedoms.

(vi) **Request restriction of processing** of your Personal data. This enables you to ask us to suspend the processing of your Personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where our use of the data is unlawful but you do not want us to erase it;
- where you need us to hold onto the data even if we no longer require it, as you need it to establish, exercise or defend legal claims; or
- where you have objected to our use of your Personal data, but we need to verify whether we have to override legitimate grounds to use it.

(vii) **Request the transfer (data portability)** of your Personal data to you or to a third party. We will provide to you, or a third party you have chosen, your Personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information that you initially provided consent for us to use or where we used the information to perform a contract with you.

(viii) **Withdraw your consent at any time** where we are relying on consent to process your Personal data (which will generally not be the case). This will **not** however affect the lawfulness of any processing which we carried out before you withdraw your consent. Any processing activities that are not based on your consent will remain unaffected.

Kindly note that none of these data subject rights are absolute, and must generally be weighed against our own legal obligations and legitimate interests. If a decision is taken to override your data subject request, you will be informed of this by our data protection team along with the reasons for our decision.

Complaints

You have the right to complain at any time to a competent supervisory authority on data protection matters, such as (in particular) the supervisory authority in the place of your habitual residence or your place of work.

We would, however, appreciate the opportunity to deal with your concerns before you approach the supervisory authority, so please contact us in the first instance at legal@rival.finance

10. Conclusion

We reserve the right to make changes to this Policy in the future, which will be duly notified to you. If you have any questions regarding this Policy, or if you would like to send us your comments, please contact us today or alternatively write to our data protection team using the details indicated in this Policy.

TERMS AND CONDITIONS OF PAYMENT CARDS

1. General Provisions

These Terms and Conditions of Payment Cards constitute a legally binding agreement between the Card Issuer (as defined below) and you ("Cardholder") which enters into force on the date the Cardholder signs a confirmation to be bound under this Agreement (by hand or electronic means) and remains in force an indefinite period of time unless it is terminated following the provisions set forth herein.

Choise Services UAB ("Partner") represent Card Issuer in the relationships with the Cardholder. Terms and conditions for financial services provided to the Client/Cardholder other than set out in these Payment Card Terms and Conditions are governed by the General Terms and Conditions r ("Terms and conditions"), which are available at https://rival.finance/ and/or in the App.

2. Definitions

2.1. The following definitions are used:

2.1.1. Account – an account opened and maintained for the Client;

2.1.2. Application – an application submitted to Card Issuer by the Client in order to order the Card;

2.1.3. Business Day(s) – any day other than a Saturday or a Sunday or a public or bank holiday in Lithuania;

2.1.4. Card – a payment instrument which has been issued by the Card Issuer to the Cardholder and owned by the Card Issuer. The term may refer to both physical items such as plastic or metal cards and sets of data such as virtual cards or digital cards (tokens);

2.1.5. Card Data - includes the name of the Cardholder, the number, validity period, and security feature (e.g., CVV code) of the Card.

2.1.6. Card Issuer – any bank or financial institution that is a member of a Card Association and issues a Card. In the relationship with the Client, Reap Technologies Limited is the Card Issuer;

2.1.7. Cardholder – a person to whom the Card is issued to and who is authorized to use the card. In the context of this Agreement the Cardholder and the Client can be the same person;

2.1.8. Client – means a customer of Partner, natural person or legal entity accepting the Partner's Terms and Conditions and its integral parts;

2.1.9. Fees – fees for issuing a Card, currency exchange, operations fees and Payment Transactions, including but not limited to. Fees and limits are publicly available in the App and/or at .

2.1.10. Directive 2015/849 – on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;

2.1.11. Partner – a third-party with whom Card Issuer has agreed to cooperate in the Distribution of Cards;

2.1.12. International Card Organization – international payment card organizations VISA International;
2.1.13. Means of Authentication – the Cardholder data, the Card data (PAN, CVC2 or CVV2, expiration date), PIN code and/or other means provided to the Cardholder by the Card Issuer that enable the Cardholder to be authenticated and operations initiated, including, but not limited to remote Payment Transactions initiated online;
2.1.14. Payment Transaction – deposit, transfer or withdrawal of funds initiated by the Payer, on behalf of the Payer or the Payee, regardless of the responsibilities of the Payer and the Payee underlying the operation;
2.1.15. Terms and Conditions of Payment Cards / Agreement – agreement concluded between the Client and Card Issuer;
2.1.16. Payee – natural or legal person who is the recipient of funds;
2.1.17. PIN – Personal Identification Number;
2.1.18. System – an electronic system used for the provision of services accessible via means of remote communication or the Internet.
2.1.19. Reap Technologies Limited - a company incorporated in Hong Kong with company registry number 2714427.
2.1.20 Virtual Card – a Card consisting of digital Card Data, and not having a physical body.
2.2. Other terms and acronyms shall have the same meaning as defined in the Partner's Terms and Conditions.

3. Client's obligations
3.1. The Client has the following obligations:
3.1.1. to observe the procedures and instructions provided by Card Issuer and requirements described in the General Terms and Conditions and its integral parts;
3.1.2. to inform Card Issuer of any malfunctions that prevent performing Payment Transactions;
3.1.3. to hold sufficient amount of Funds on the Account to settle Commission Fees and carry out Payment Transactions;
3.1.4. to immediately but no later than in 5 (five) Business Days notify Partner if any material information on the Cardholder has changed;
3.1.5. inform and ask the Partner to block the Card immediately after the Card was stolen, lost, third-parties have learned the Means of Authentication.

4. Card issuing
4.1. To receive the Card, the Client must submit an Application to Card Issuer via the System or a Partner.
4.2. Card Issuer, after accepting the Client's Application, shall issue a Card. If the Client requests, Card Issuer may issue multiple Cards. Card Issuer shall solely at its own discretion determine the total number of issued Cards.
4.3. At the Client's request, the Card may be issued not only to the Client, but also to another person indicated by the Client with an approval of the Client, i.e. a Cardholder. If the Client

requests to issue a Card to another person, the Client must inform the Cardholder of the conditions set in the Agreement.
4.4. The Cardholder, after issuing the Card shall be provided with unique Means of Authentication (e.g. CVV code, and/or PIN code for the Chip&Pin Card). Such Means of Authentication are considered as the Cardholder's signature in order to perform Payment Transactions. The use of the Means of Authentication shall mean the consent and authorization to perform Payment Transactions.
4.5. The Cardholder shall not disclose Means of Authentication to third-parties.
4.6. Card Issuer has the right to send the Card and the Means of Authentication by post or through Card Issuer authorized person. Upon receipt of the physical Card, the Cardholder is obliged to make sure that the envelope with the Card and its Means of Authentication have not been opened nor damaged. The physical Card is activated either in the App of the Partner or in the other environment provided by the Partner.
4.7. The Virtual Card consists only of the Card Data, the physical card is not issued. The transfer of Card Data and activation takes place in the App or in the other environment provided by the Partner.
4.8. The Cardholder may start performing Operations once the Card has been activated.

5. Card payments
5.1. Only the Cardholder has the right to perform Payment Transaction with the Card.
5.2. Payment Transaction may be performed by the Cardholder:
5.2.1. immediately after a virtual Card is issued;
5.2.2. only after a physical Card in accordance with the received instructions has been activated.
5.3. The Cardholder may perform Payment Transaction only within the amount located on the Account and in accordance with the Card usage limits (daily, weekly, monthly maximum amount for Payment Transactions) indicated in the Agreement. Card Issuer reserves the right to determine Card usage limits.
5.4. Card Issuer assumes that all Payment Transactions are consented to, authorised and initiated by the Cardholder, unless proven otherwise.
5.5. The use of the Card or Means of Authentication to initiate a Payment Transaction shall be considered as an authorisation and consent to carry out the Payment Transaction. Unless established differently for the protection of consumer rights, if the Cardholder provides consent to perform a Payment Transaction, the Cardholder is not entitled for a refund unless the Payee agrees to refund the transferred amount to the Cardholder.
5.6. Payment transactions initiated using the Card will be executed in the Account according to the Agreement and General Terms and Conditions, its integral parts and the applicable law.
5.7. Payment Transaction performed by the Cardholder using the Card may be declined if:
5.7.1. the Card is invalid or blocked (in accordance with Section 7);
5.7.2. Card Issuer has closed, suspended or restricted the use of the Client's Account;
5.7.3. the amount of Funds needed to perform the Payment Transaction exceeds the available

amount of Funds on the Client's Account;
5.7.4. any other basis which arises from the Agreement or legal acts or the Client is suspected of fraud/illegal activities.
5.8. Card Issuer reserves the right to use third-parties provided services in order to ensure the execution of Payment Transaction or any other services.
5.9. At the request of the Partner and/or Card Issuer, the service provider (e.g. e-shops) may refuse to accept payment with the Card.
5.10. The Client and/or the Cardholder has the right to request that the Card be blocked and/or closed at any time.
5.11. A blocked, closed, or invalid Card may not be used.
5.12. Card Issuer has the right to determine the Card limits and the minimum and maximum amount of a one-off Payment Transaction. Partner shall have the right to set other limits for its client, provided that it does not contradict minimum and maximum limits set by Card Issuer.

6. Requirements for ensuring a secure Card usage
6.1. The Cardholder ensures:
6.1.1. to active the physical Card before usage. This process has to be proceeded after receiving the physical Card. The Cardholder shall be liable for any damages to the Card due to premature activation or not following the Card activation instructions.
6.1.2. to protect the physical Card from any physical damage including copying, modification etc.;
6.1.3. not to provide the Card to third-parties unless the third-party is accepting the payment;
6.1.4. not to use the Card for illegal activities, including purchases of goods/services which are prohibited by applicable law;
6.1.5. to immediately report any malfunctions which may influence the performance of Payment Transactions;
6.1.6. to follow any other obligations stated in the Agreement.
6.2. The Cardholder has the obligation to keep the Card and the Means of Authentication secure. The Cardholder shall restrain from recording the Means of Authentication on any information carriers which may be used by third-parties in order to gain access to the Card or the Means of Authentications.
6.3. Card Issuer upon receiving information that the Card is used by third-parties and not by the Cardholder shall take necessary measures to block the Card.
6.4. If a third party has learned the Card Data and in any other case when there is a risk of a third party using the Card, the Cardholder shall immediately inform the Partner by using the phone number and the business hours shown on the Partner's Website and/or the App.

7. Validity and Card blockage
7.1. The Card is valid inclusively until the last day of the calendar month stated on the Card. As

soon as the next calendar month begins after the calendar month stated on the Card, the Card shall be deemed invalid.
7.2. If the Account was closed, the Card is considered expired (invalid) and, therefore, no longer valid from the moment the Account was closed.
7.3. In order to verify circumstances of Card use, Card Issuer reserves the right to block the usage of the Card if:
7.3.1. Means of Authentication have been disclosed to persons who have no right to use the Card;
7.3.2. the Account is closed, suspended or restricted;
7.3.3. Cardholder's activities performing Payment Transactions may be associated with fraud or any other illegal activities;
7.3.4. obligations are not duly performed by the Cardholder;
7.3.5. other grounds which are deemed important for blocking the Card.
7.4. If reasons for Card blocking remain, Card Issuer has the right to block the Card.
7.5. Cardholder has the right to request the Card to be blocked at any time.
7.6. In events when the Cardholder enters the PIN incorrectly three times in succession, the physical Card will be blocked. In such case the Cardholder shall inform Card Issuer or the Partner immediately.
7.7. Card Issuer shall not be liable for any type of damages caused to the Cardholder or other third-parties for Card blockage, unless legal acts determine otherwise.

8. Card Issuer rights in conjunction with prevention of money laundering and terrorism financing
8.1. Card Issuer in accordance with Directive 2015/849 and implementing legislation has the following rights:
8.1.1. to exchange information and documents of the Cardholder to ensure the prevention of money laundering and terrorist financing;
8.1.2. to regularly verify the information on identification of the Cardholder and at any moment request the Cardholder to submit additional documents;
8.1.3. to apply temporary or permanent restriction on Cardholder's performing Payment Transactions;
8.1.4. to request documents and information of any kind regarding the Cardholders activities;
8.1.5. to request documents and information of any kind regarding persons involved in the transaction;
8.1.6. to request any other type of documents and information which are required by Card Issuer to ensure the duty in prevention of money laundering and terrorism financing;
8.1.7. to refuse the execution of Payment Transactions if the Cardholder does not comply with the requirements preventing money laundering and terrorist financing.

9. Liability

9.1. The Cardholder is liable for the breach of obligations stated in the Agreement, General Terms and Conditions, its integral parts or any other legal acts.
9.2. Card Issuer shall not be held liable for the involvement of third-parties in processing the Payment Transactions. Card Issuer does not take responsibility of third-parties for the refusal to accept the Card in order to pay for goods or services.

10. Fees
10.1. The Cardholder shall pay Fees for the issuance of the Card including postal expenses described in the App and/or at https://vault.rival.finance/ or otherwise agreed between the Parties.
10.2. All Fees for the Payment Transactions shall be debited by Card Issuer or Partner from the Account.
10.3. Currency conversion fees are specified in the Cardholder's Account and currency exchange is based on the exchange rate of International Card Organizations that are publicly available and are valid at the time of conversion.
10.4. Card Issuer decision to block the Card shall not be considered as termination of the Agreement and General Terms and Conditions or other integral parts. Therefore, the act of blocking of the Payment Card, i.e. refusal to carry out Payment Transactions, shall not free the Cardholder from Commission Fee calculation of provided services or lift the obligation to pay calculated Commission Fees.

11. Final provisions
11.1. All relationships between the Client, the Cardholder, the Partner and Card Issuer are governed by the laws of the Republic of Lithuania.
11.2. Card Issuer has the right to disclose information about the Payment Transactions performed by the Cardholder to third-parties, who under legal acts have the right to receive such information.
11.3. Agreement may be amended or terminated by giving the Client at least 60 (sixty) day written notice thereof. Within these 60 (sixty) days, the Client has the right to terminate Agreement with immediate effect and free of charge provided that all the obligations arising from the Payment Card Terms and Conditions have been fulfilled. If the Client has not terminated the Payment Card Terms and Conditions within the period specified above, he shall be deemed to have accepted the amendments.
11.4. The Client has the right to terminate the Agreement by giving at least 30 (thirty) day notice thereof.
11.5. Card Issuer has the right terminate the Agreement as an extraordinary remedy without giving advance notice if:
11.5.1. The Client and/or the Cardholder has provided false information to Card Issuer and/or Partner when applying for the Card or has failed to provide information known to the Client

and/or the Cardholder affecting the performance of the Agreement;
11.5.2. (Not applicable to the Clients and the Cardholders who are consumers) The Client has failed to fulfil his payment obligation owed to Partner within an additional term of 14 (fourteen) days given to the Cardholder and Partner has made a relevant request;
11.5.3. The Card issued hereunder has been closed and/or blocked for at least four (4) consecutive months;
11.5.4. (Not applicable to the Clients and the Cardholders who are consumers) The Card has not been used for Operations for six (6) consecutive months.
11.6. The termination of the Agreement shall not affect the collectability or satisfaction of financial claims arising prior to the termination of the Agreement.
11.7. This Agreement shall be published on website at https://rival.finance/
11.8. Personal data processing is made in accordance with the Privacy Policy of available on website at https://rival.finance/pdf/rival-privacy-policy.pdf

Last updated: 1st March 2024

Terms of Exchange Operations

NOTE: Exchange operations with cryptocurrencies involve a high degree of risk. Values of cryptocurrencies are subject to fluctuation and there is a significant time lag between placement of your exchange Order and delivery of cryptocurrency to your account.

By submitting the Order, you will be deemed to have accepted these Terms of Exchange Operations and Terms of Use (available on our website https://rival.finance/).

If you do not yet have an Account, then an Account will be opened for you at the time of your submission of the Order using the details that you will have submitted and you will be treated as a Client from such time. You may be required to undergo applicable KYC procedures before your Order can be processed.

1. GLOSSARY OF TERMS

1.1. The website and mobile apps are owned by the company RIVAL PAYMENTS SERVICES PROVIDER LLC, incorporated in United Arab Emirates with a registered number 1308095 and registered office at Dubai, Business Bay, Burlington Tower, Office 403 **("Rival Finance").**

1.2. Choise Services UAB, a legal entity duly registered in Lithuania with No. 305964183 with a registered office at Vokieciu gatve 18a-7, Vilnius ("**Company**") or any successor or assignee thereto.

1.3. Charism LLC of Suite 336, Beachmont Business Centre, Kingstown, St. Vincent, and Grenadines, registration number 1999 LLC 2022, is a limited liability company created and existing under the laws of Saint Vincent and Grenadines ("**Choise**", "we", "us")

1.4. Account – the Client's account with Rival Finance.

1.5. Business Day – any day on which banks are open for business in Saint Vincent and Grenadines.

1.6. Client – a User as such term is defined in Terms of Use.

1.7. Commission – the Exchange's commission for the Exchange Operation

1.8. Conversion Estimate – the estimated amount of Tokens that the Exchange may be able to purchase with the Invoice Amount (minus the Trade Commission), subject to any fluctuation in the purchase price of Tokens

1.9. ID – the Client's Company identification/client number

1.10. Exchange – Company or any successor or assignee thereto

1.11. Exchange Operation – the exchange of the Client's Euro funds into Tokens

1.12. Hotline – the customer service hotline is available via support@rival.finance

1.13. Invoice – the Exchange's invoice to the Client for the Exchange Operation

1.14. Order – the Client's order for the Exchange Operation submitted to the Exchange electronically and setting out the amount of Euro funds the Client instructs the Exchange to exchange into Tokens Tokens – USDT (Tether) tokens (tether.io)

1.15. Refund commission – commission charged in case of can refund.

1.16. Trade Commission – the Exchange's commission for carrying out the Exchange Operation. For the current Trade Commissions, please refer to the Fee Schedule

1.17. Trade Confirmation – a confirmation sent to the Client by Exchange confirming the receipt of the Order Transaction rollback – commission charged for cancellation of the inner transaction.

2. LIMITS

2.1. Your monthly Orders may not exceed **150.00 Euro** until your Client account

satisfies applicable KYC1 requirements.

2.2. After satisfaction of applicable KYC1 requirements, the following limits apply[1]:

- Maximum amount of one transaction: 3,000 EUR
- Maximum daily quantity of purchases per bank card: 4
- The maximum daily amount of purchases per bank card: 10 000 EUR
- The maximum monthly amount of purchases per bank card: 15 000 EUR

3. OPERATION RULES

3.1. To initiate the Exchange Operation, the Client must place the Order.

3.2. After placing the Order, the Client will get a Trade Confirmation and will be invoiced by the Exchange for the full amount of the Order. The Invoice will be delivered to the Client electronically via email provided by him/her and a copy of the Invoice will also be available for download through the Client's Account.

3.3. The Trade Confirmation will contain the Conversion Estimate and will state the amount of the Trade Commission.

3.4. The Invoice should be paid by the Client by wire transfer in immediately available funds by the close of the Business Day immediately following the date of the Invoice. For purposes of this paragraph, 'payment' means the irrevocable debit of the Client's Euro account with the Client's bank (credit institution) that maintains such account, for the full amount of the Invoice, based on an irrevocable instruction by Client to such bank to transfer and pay the net amount stated in the Invoice ("**Invoiced Amount**") to the Exchange.

3.5. The Invoiced Amount should be paid to the Exchange in full. Payment of all commissions, transfer fees, duties, and other expenses associated with payment of the Invoiced Amount is the Client's expense and responsibility.

3.6. After receipt of the Invoiced Amount, the Exchange will deduct its Trade Commission from the Invoiced Amount and will use the remaining funds to purchase and deliver the Tokens to the Client's Account.

3.7. The Client's payment instructions must include a reference to the Client's ID. Failure to include such reference may result in delays in (a) processing of the Order by the Exchange and (b) purchase and delivery of the Tokens by the Exchange to the Client and, accordingly, the Client may not receive the Tokens in time or at all, which may result in various losses to the Client.

3.8. The Company has to identify you as a cardholder, an individual who is issued and authorized to use a card, to be compliant with applicable anti-fraud requirements. To prevent fraud and the misuse of funds, the Company needs to ensure that the card used for payment belongs to the Account holder. In the situation where the Company's staff has a reason to make any additional checks, the staff member may request additional supporting materials from the account holder.

If the amount received by the Exchange according to the Invoice is less than the full Invoiced Amount ("**Insufficient Amount**"), the Exchange will advise the Client accordingly and the Client may instruct the Exchange (through the Hotline) to amend the Order to be equal to such Insufficient Amount. Such an amendment will not diminish the amount of the Trade Commission established in the Trade Confirmation.

If no such instruction is received within 5 (five) Business Days from the date of receipt of such Insufficient Amount by the Exchange, the Exchange will initiate a remittal of the excess (minus all applicable bank commissions, charges, and duties) by wire transfer to Client.

3.9. If the amount received by the Exchange according to the Invoice is higher than the

[1] In case the payment currency differs from the euro, the applicable limits are calculated in euro equivalent in accordance with the current exchange rate of the processing partner

full Invoiced Amount ("**Excessive Amount**"), the Exchange will advise the Client accordingly and the Client may instruct the Exchange (through the Hotline) to issue an additional Invoice for the excess. In such case, a separate Trade Commission will apply to such additional Invoice.

If no such instruction is received within 5 (five) Business Days from the date of receipt of such Excessive Amount by the Exchange, the Exchange will initiate a remittal of the excess (minus all applicable bank commissions, charges, and duties) by wire transfer to Client.

3.10. The Conversion Estimate of the Trade communicated to the Client after placement of the Order is indicative and, although we usually intend to fill the Order at the best available Token price, the actual amount of Tokens that may be delivered to the Client according to the Order may vary. This variance is due to several factors such as:

a) The purchase of Tokens by Exchange according to the Order only takes place after the Exchange receives the Invoice payment in full.
b) Accordingly, the purchase price (market value) of the Token may go up or down between the time the Client makes the Invoice payment, the time the Exchange receives the Invoice payment, and the time the Exchange purchases and delivers the Tokens to the Client.
c) There may be market disruptions, regulatory changes, or other adverse effects on the Tokens and the market for the Tokens which may affect their availability, recording, circulation, value, or deliverability to the Client.

3.11. Please note that in case of a chargeback, we do not return to the Client any sum paid by you as a commission for making the transaction.

4. BASIC FEE SCHEDULE FOR PURCHASE VIA BANK CARD

Order Value up to and including	**Trade Commission**
EUR 1 000.00	8.00%
EUR 10 000.00	7.50%
EUR 100 000.00	7.00%
EUR 1 000 000.00	6.50%

4.1. The company reserves the right to apply to Lower Trade Commission at its consent without additional notice.

4.2. Coins that are not convinced to be used in the mobile app but can transfer in blockchain to a valid e-wallet in the mobile app are lost. The Company cannot transfer them back to the Clients.

4.3. The client is informed and taking into account that he or she will be charged in the amount of 10 Euro for every mistaken transaction made by him or her in the mobile application unless the bigger amount is not contemplated by other paragraphs of this Terms or any other agreements you are bound with the Company.

4.4. The Company does not guarantee a refund in case of wrong mentioning token tag which causes to depositing of coins into the user account as well as to transferring of coins to an e-wallet that is outside of the mobile application and whose holder is not the one who legally bound with the Company. If in any case, the Company was

successful in making such a refund the Client is charged with a commission of 35 Euro.

4.5. The Company does not make a refund if the transaction was successfully completed (i.e. exchange of digital assets was done, the Client closed the deal with the merchant (bought goods, received services, and so on), etc.), unless such transaction was made due to fraudulent actions of third persons and criminal activity of any kind.

4.6. The funds are to be transferred to the address (including each component of it) mentioned in the application for a digital asset which is managed especially in the main network of a specified blockchain.

4.7. **Company and/or is not obliged for loss of funds in case of non-obligation of the conditions mentioned above in this paragraph and also in the following cases:**

a) Mentioning the wrong tag for the transfer of funds (including XRP);
b) Transaction made to the wrong address or to address in another blockchain;
c) ERC-20 transaction made to smart-contract address;
d) Other similar cases.

Thus, in such cases, no refund is contemplated.

4.8. We also note that the use of nonofficial client applications or algorithms for the operation of services offered by the Company is strictly prohibited. The Company is entitled to recover several funds if for wealth accumulation you took advantage of technical mistakes and system failure, i.e.:

a) Making exchange at the wrong rates;
b) Using of trial-and-error method;
c) Using custom programs, and third-party services to turn to account a technical vulnerability.

Last updated: 1st March 2024

Rival Finance General Terms of Use

PLEASE READ THESE GENERAL TERMS OF USE CAREFULLY BEFORE ACCEPTING THEM (BEFORE AGREEING TO THE CONDITIONS CONTAINED IN THEM). BY CLICKING THE "CREATE ACCOUNT" BUTTON OR BY ACCESSING OR USING THE SERVICES, YOU AGREE TO BE LEGALLY BOUND BY THESE GENERAL TERMS OF USE AND ALL TERMS INCORPORATED BY REFERENCE.

BY MAKING USE OF SERVICES, YOU ACKNOWLEDGE AND AGREE THAT: (1) YOU ARE AWARE OF THE RISKS ASSOCIATED WITH TRANSACTIONS OF DIGITAL CURRENCIES AND/OR ASSETS; (2) YOU SHALL ASSUME ALL RISKS RELATED TO THE USE OF SERVICES AND TRANSACTIONS OF DIGITAL CURRENCIES AND THEIR DERIVATIVES; AND (3) RIVAL FINANCE SHALL NOT BE LIABLE FOR ANY SUCH RISKS OR ADVERSE OUTCOMES.

BY ACCESSING AND USING SERVICES, YOU REPRESENT AND WARRANT THAT YOU HAVE NOT BEEN INCLUDED IN ANY TRADE EMBARGOES OR ECONOMIC SANCTIONS LIST (SUCH AS THE UNITED NATIONS SECURITY COUNCIL SANCTIONS LIST), THE LIST OF SPECIALLY DESIGNATED NATIONALS MAINTAINED BY OFAC (THE OFFICE OF FOREIGN ASSETS CONTROL OF THE U.S. DEPARTMENT OF THE TREASURY), OR THE DENIED PERSONS OR ENTITY LIST OF THE U.S. DEPARTMENT OF COMMERCE. WE RESERVE THE RIGHT TO CHOOSE MARKETS AND JURISDICTIONS TO CONDUCT BUSINESS AND MAY RESTRICT OR REFUSE THE PROVISION OF SERVICES IN CERTAIN COUNTRIES OR REGIONS.

This General Terms of Use applies to customers residing outside the "Prohibited Jurisdictions," details of which can be found at https://vault.rival.finance/.

1. Acceptance of the General Terms of Use

1.1. These General Terms of Use are entered into by and between you and **Choise Services UAB**, a legal entity duly registered in Lithuania with 305964183 with a registered office at Vokieciu gatve 18a-7, Vilnius, ("Choise", "we", "us"), and **Charism LLC**, a limited liability company, incorporated in St. Vincent and Grenadines with company number 1999 LLC 2022, registered office at Suite 336, Beachmont Business Centre, Kingstown, St. Vincent, and Grenadines, and **Crypterium AS**, a legal entity duly registered in Estonia with No. 14352837, registered office at Harju maakond, Tallinn, Kesklinna linnaosa, A. Lauteri tn 5, 10114 (“Associated companies”).

1.2. The Website and Mobile Applications are owned by the company RIVAL PAYMENTS SERVICES PROVIDER LLC, incorporated in United Arab Emirates with a registered number 1308095 and registered office at Dubai, Business Bay, Burlington Tower, Office 403 **("Rival Finance")**.

1.3. By using the Website or any Services or by clicking to accept or agree to the Terms of Use when this option is made available to you, you accept and agree to be bound and abide by these Terms of Use in addition to

- our Privacy Policy, incorporated herein by reference; and
- our Cookie Policy, incorporated herein by reference; and
- our KYC/AML Policy, incorporated herein by reference; and
- our Anti-fraud Policy, incorporated herein by reference; and
- our Terms of Exchange Operations, incorporated herein by reference; and

- our IP notice, incorporated herein by reference.

1.4. The following terms and conditions, together with any documents they expressly incorporate by reference (collectively, these "Terms of Use"), govern your access to and use of https://rival.finance/ ("Website"), including any associated mobile applications (“Applications”) and your access to and use of any media, analytics, content, functionality, and services offered on or through any of the Website and Applications, and your access to and use of all and any related sites and services. The Website, the Applications, and all and any other media, analytics, content, functionality, Services, and services offered by us or through us, are referred to as the “Services”. If you do not agree to these Terms of Use, you must not access or use the Website and any Services or any Application or access or use any Services.

2. Usage Requirements

2.1. The Website is offered and available to users who are of legal age (i) in Saint Vincent and Grenadines (18 years or older) and (ii) in the users’ jurisdiction or place of residence.

2.2. By using a Website and any Services, you represent and warrant that you (i) are 18 years of age or older, (ii) are of legal age in your jurisdiction or place of residence, (iii) are not barred from using the Website and any Services under any applicable law, order, directive, regulation, or sanction list and (iii) are using the Website and any Services only for a lawful purpose.
If you do not meet these requirements, you must not access or use the Website and any Services.

2.3. As a Client, that is a legal entity, on behalf of such legal entity you represent and warrant that (i) such legal entity is duly organized and validly exists under the legislation of the jurisdiction of its organization; (ii) you are duly authorized by such legal entity to act on its behalf; and (iii) this legal entity is not registered in the Prohibited Jurisdictions, as well as the beneficial owners of this legal entity are not citizens (nationals) of the countries that are in the list of Prohibited Jurisdictions and do not reside in the Prohibited Jurisdictions.

3. Content and its intended use

3.1. We may change the format and content of the Website and the Services from time to time without noticing you. You agree that your use of the Websites and the Services is on an 'as is' and 'as available' basis and is at your sole risk.

3.2. Whilst we try to make sure that all information contained in the Websites and any Services (other than any user-generated content) is correct, it is not, and it is not intended to be, any authority or advice on which any reliance should be placed.

4. Reliance on Information Posted

4.1. The information presented on or through the Websites and any Services is made available solely for general information purposes. We do not warrant the accuracy, completeness, or usefulness of this information. Any reliance you place on such information is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on such materials by you or any other visitor to the Websites, or by anyone who may be informed of any of its contents.

4.2. The Website and any Services may include content provided by third parties, including materials provided by other users, bloggers, and third-party licensors, syndicators, aggregators, and/or reporting services. All statements and/or opinions expressed in these materials, and all articles and responses to questions and other content, other than the content provided by the Company, are solely the opinions and the responsibility of the person or entity providing those materials. These materials do not necessarily reflect the opinion of the Company. We are not responsible, or liable to you or any third party, for the content or accuracy of any materials provided by any third parties.

4.3. The Website and the Services are not in any manner or in any form or part intended to constitute or form the basis of any advice (professional or otherwise) or to be used in, or about, any investment or other decision or transaction.

4.4. We do not accept any liability (regardless of how it might arise) for any claim or

loss arising from:

- any advice given;
- any investment or other decision made; or
- any transaction made or effected;
- in reliance on, or based on, any information on the Websites or in any of the Services, nor do we accept any liability arising from any other use of, or reliance on, the Services.

4.5. We do not enter into any terms or make any representations as to the accuracy, completeness, currency, correctness, reliability, integrity, quality, fitness for purpose, or originality of any content of the Websites and the Services and, to the fullest extent permitted by law, all implied warranties, conditions or other terms of any kind are hereby excluded. To the fullest extent permitted by law, we accept no liability for any loss or damage of any kind incurred as a result of you or anyone else using the Websites and the Services or relying on any of its content.

4.6. We cannot and do not guarantee that any content of any Website and any Services will be free from viruses and/or other code that may have contaminated or destructive elements. It is your responsibility to implement appropriate IT security safeguards (including antivirus and other security checks) to satisfy your requirements for the safety and reliability of content.

5. Changes to the Terms of Use

5.1. We may revise and update these Terms of Use from time to time at our sole discretion. All changes are effective immediately when we post them.

5.2. Your continued use of the Websites and any Services following the posting of revised Terms of Use means that you accept and agree to the changes. You are expected to check this page frequently, so you are aware of any changes, as they are binding on you.

6. Accessing the Websites

6.1. We reserve the right to withdraw or amend this Website, and any service or material we provide on the Website and any Services, in our sole discretion without notice. We do not guarantee that our Website or any content on it will always be available or will not be interrupted. We will not be liable if for any reason all or any part of the Websites and any Services is unavailable at any time or for any period. From time to time, we may restrict access to some parts of the Websites and any Services, or an entire Website, to users.

6.2. You are responsible for:

- Make all arrangements necessary for you to have access to the Websites and any Services.
- Ensuring that all persons who access the Websites and any Services through your internet connection are aware of these Terms of Use and comply with them.

6.3. To access a Website or some of the resources it offers, you may be asked to provide certain registration details or other information. It is a condition of your use of the Website that all the information you provide on the Website is correct, current, and complete. You agree that all information you provide to register using a Website or otherwise, including, but not limited to, using any interactive features on the Website, is governed by our Privacy Policy, and you consent to all actions we take concerning your information consistent with our Privacy Policy.

6.4. You should use caution when inputting personal information onto Websites on a public or shared computer so that others are not able to view or record your personal information.

7. Mobile Applications

7.1. <u>Apple Application</u>

7.1.1 If the Services that you access and use is an Apple Application:

the Apple Application may be accessed and used only on a device owned or

controlled by you and using the Apple iPhone OS;

7.1. 2. You acknowledge and agree that:

- Apple has no obligation at all to provide any support or maintenance services concerning the Apple Application. If you have any maintenance or support questions concerning the Apple Application, please contact us, not Apple, using the contacting us details at the end of these Terms of Use;
- although these Terms of Use are entered between us and you (and not Apple), Apple, as a third-party beneficiary under these Terms of Use, will have the right to enforce these Terms of Use against you;
- except as otherwise expressly set out in these Terms of Use, any claims relating to the possession or use of the Apple Application are between you and us (and not between you, or anyone else, and Apple); and
- in the event of any claim by a third party that your possession or use (in accordance with these Terms of Use) of the Apple Application infringes any intellectual property rights, Apple will not be responsible or liable to you concerning that claim;

7.1.3. You represent and warrant that:

- You are not, and will not be, located in any country that is the subject of a US Government embargo or that has been determined by the US Government as a "terrorist supporting" country; and
- you are not listed on any US Government list of prohibited or restricted parties; and
- If the Apple Application that you have purchased does not conform to any warranty applying to it, you may notify Apple, which may then refund the purchase price of the Apple Application to you. Subject to that, and to the maximum extent permitted by law, Apple does not give or enter into any warranty, condition, or other term concerning the Apple Application and will not be liable to you for any claims, losses, costs, or expenses of whatever nature concerning the Apple Application or as a result of you or anyone else using the Apple Application or relying on any of its content.

7.2. Android Applications

7.2.1. If the Services that you access, and use an Android Application:

the Android Application may be accessed and used only on a device owned or controlled by you and using an Android OS;

7.2.2. You acknowledge and agree that:

- Google has no obligation at all to provide any support or maintenance services concerning the Android Application. If you have any maintenance or support questions concerning the Android Application, please contact us, not Google, using the contacting us details at the end of these Terms of Use;
- although these Terms of Use are entered into between us and you (and not Google), Google, as a third-party beneficiary under these Terms of Use, will have the right to enforce these Terms of Use against you;
- unless otherwise expressly set out in these Terms of Use, any claims relating to the possession or use of the Android Application are between you and us (and not between you, anyone else, and Google); and
- in the event of any claim by a third party that your possession or use (in accordance with these Terms of Use) of the Android Application infringes any intellectual property rights, Google will not be responsible or liable to you concerning that claim; and

7.2.3. You represent and warrant that:

- You are not, and will not be, located in any country that is the subject of a US Government embargo or that has been designated by the US Government as a "terrorist supporting" country; and
- You are not listed on any US Government list of prohibited or restricted parties.

8. Account Security

8.1. Be careful to keep your private keys, passwords, security codes, and other security features that you use to access the Services. You must maintain the security of your Account by protecting your login, password, and security credentials from unauthorized access or use. It is your responsibility to ensure the security of, and your continuous control over, any device or account that may be associated with enhanced security features. You must properly read, use, and follow the Anti-fraud policy, and notify us if you discover or suspect any unauthorized access or use of your Account or any security breaches related to your Account. Upon receipt of written notice from you that the security of your Account has been compromised, we will take reasonable steps to protect your Account.

8.2. Please note that You are responsible for all activities that occur under your Account, and by agreeing to these Terms you accept all risks of any authorized or unauthorized access to your Account. You will be bound by, and you hereby authorize us to accept and rely on, any agreements, instructions, orders, authorizations, and any other actions made, provided, or taken by anyone who has accessed or used your Account regardless of whether the access is authorized or unauthorized by you.

Please note that you may open only one Account as well as reach an agreement with other persons on joint and (or) coordinated actions on using the Accounts in a certain way (including for making a profit (generating income) or to achieve other goals). Creation of more than one Account is strongly prohibited and may lead to refusal of providing our services.

9. Trademarks

9.1. Our name, the brand “Choise.com” (application number 2022703181 as of 21.01.2022) “Choise” (application number 2022703182 as of 21.01.2022), our logo and all related names, logos, Services and service names, designs, and slogans are trademarks. You must not use such marks without prior written permission. All names, logos, Services and service names, designs, and slogans on the Websites and any Services (“**Marks**”) are the trademarks of their respective owners.

9.2. Nothing contained in the Websites or any Services should be construed as granting any license or right to use any of the Marks for any purpose whatsoever without the written permission of, or entry into the applicable license terms with, the lawful owner. Unauthorized use of the Marks or any information is strictly prohibited and may violate trademark, copyright, or other applicable laws. In the event you print off, copy, or store any of our content (which you may do only as permitted by these Terms of Use), you must ensure that any copyright, trademark, or other intellectual property right notices contained in the original content are reproduced.

10. Services

10.1. Charism LLC provides the following services following this Terms of Use:

Providing services for opening the User Account
Providing services for exchanging one crypto asset for another one
Providing services for crypto credits
Providing services for crypto savings, including dual currency deposits.

The Charism LLC is not responsible and does not assume any liability whatsoever for acts, errors, or omissions of any third party.

10.2. Choise Services UAB provides the following services following this Terms of Use:

Providing services for exchanging crypto assets to fiat and vice versa (including insured exchange operations)

The Choise Services UAB is not responsible and does not assume any liability whatsoever for acts, errors, or omissions of any third party.

10.3. Crypterium AS provides the following services in accordance with these Terms of Use:

Providing services registration and onboarding of users, Providing services of implementation Anti-Money Laundering/Know Your Customer principles on Website

10.4. We may share your personal data with third parties for purposes of providing services described in this Clause. Please check our Privacy Policy for more details.

11. Prohibited Uses

11.1. You may use the Websites and any Services only for lawful purposes and in accordance with these Terms of Use. You agree not to use the Websites and any Services:

- In any way that violates any applicable national, regional, local, or international law or regulation (including, without limitation, any laws regarding the export of data or software to and from the EU or other countries).
- For the purpose of exploiting, harming, or attempting to exploit or harm minors in any way by exposing them to inappropriate content, asking for personally identifiable information, or otherwise.
- To send, knowingly receive, upload, download, use, or re-use any material which does not comply with these Terms of Use.
- To transmit, or procure the sending of, any advertising or promotional material without our prior written consent, including any "junk mail", "chain letter" "spam" or any other similar solicitation.
- To impersonate or attempt to impersonate the Company, a Company employee, another user, or any other person or entity (including, without limitation, by using email addresses or screen names associated with any of the foregoing).
- To engage in any other conduct that restricts or inhibits anyone's use or enjoyment of the Websites and any Services, or which, as determined by us, may harm the Company or users of the Websites and any Services or expose them to liability.

Additionally, you agree not to:

- republish, redistribute, or re-transmit any data from any of our communications, analytics, and other Services without our permission;
- copy or store any of our Services other than for your personal non-commercial use and as may occur incidentally in the normal course of use of your browser or mobile device;
- store any Services (including pages of a Website) on a server or other storage device connected to a network or create a database by systematically downloading and storing any data from the Website or the Services;
- remove or change any content of any Services or attempt to circumvent security or interfere with the proper working of the Services or any servers

on which it is hosted;

- create links to a Website from any other website, without our prior written consent, although you may link from a website that is owned and operated by you provided that (a) the link is not misleading or deceptive and fairly indicates its destination, (b) you do not state or imply that we endorse you, your website, or any Services or services you offer, (c) you do not create any misimpression or confusion among users concerning sponsorship or affiliation, (d) you link only to the home page of the Website and (e) the linked website does not contain any content that is unlawful, threatening, abusive, libelous, pornographic, obscene, vulgar, indecent, offensive or which infringes on the intellectual property rights or other rights of any third party;
- use the Websites or any Services in any manner that could disable, overburden, damage, or impair the site or interfere with any other party's use of the Websites and any Services, including their ability to engage in real-time activities through the Website and any Services;
- use any robot, spider, or other automatic device, process, or means to access the Websites for any purpose, including monitoring or copying any of the material on the Websites;
- create (whether for yourself or someone else) any financial Services or service which seeks to match the performance of or the capital or income value of which is related to, any of our Services or services;
- use any manual process to monitor or copy any of the material on a Website or for any other unauthorized purpose without our prior written consent.
- use any device, software, or routine that interferes with the proper working of a Website.
- introduce any viruses, trojan horses, worms, logic bombs, or other material that is malicious or technologically harmful.
- attempt to gain unauthorized access to, interfere with, damage, or disrupt any parts of a Website, the server on which the Websites are stored, or any server, computer, or database connected to any Website.
- attack any Website via a denial-of-service attack or a distributed denial-of-service attack.
- otherwise, attempt to interfere with the proper working of the Website.

Except to the extent expressly set out in these Terms of Use, you are not allowed to:

- otherwise, do anything concerning any of the Services that is not expressly permitted by these Terms of Use.
- You must use the Websites and the Services, and anything available via such, only for lawful purposes (complying with all applicable laws and regulations), in a responsible manner, and not in a way that might damage our name or reputation or that of any of our affiliates.
- All rights granted to you under these Terms of Use will terminate immediately if you breach or fail to comply with any of these Terms of Use.
- To do anything with the Websites and the Services that are not expressly permitted by these Terms of Use, you will need a separate license from us. Please contact us via support@rival.finance

12. Changes to the Website

12.1. We may update the content on any Website and any Services from time to time,

but its content is not necessarily complete or up-to-date. Any of the material on any Website or in any Services may be out of date at any given time, and we are under no obligation to update such material.

13. Information About You and Your Visits to the Websites

13.1. All information we collect on this Website is subject to our Privacy Policy. By using the Website, you consent to all actions taken by us concerning your information in compliance with the Privacy Policy.

14. Confidential Information

14.1. When using a Website or any Services, data may be transmitted over an open network which may allow such communications to be intercepted by third parties. As a result, we cannot guarantee the confidentiality or security of any communication or data that you may transmit to us through the Websites.

15. Other Terms and Conditions

15.1. Additional terms and conditions may also apply to specific services or features of the Websites and any Services, including the promo rules in respect to the promotional events, public competitions and other event. All such additional terms and conditions are hereby incorporated by this reference into these Terms of Use.

16. Links from the Websites

16.1. If a Website contains links to other sites and resources provided by third parties, these links are provided for your convenience only. This includes links contained in advertisements, including banner advertisements and sponsored links. We have no control over the contents of those sites or resources and accept no responsibility for them or for any loss or damage that may arise from your use of them. If you decide to access any of the third-party websites linked to any Website, you do so entirely at your own risk and subject to the terms and conditions of use for such websites. We reserve the right to withdraw linking permission without notice.

17. Third party services

17.1. Certain features of our Websites and Services may utilize the services and/or Services of third-party vendors and business partners, which services and/or Services may include software, information, data or other services. Certain of these vendors and business partners require users who utilize such features to agree to additional terms and conditions. This page identifies third-party terms and conditions that are required by such third-party vendors and business partners as they apply to the features set forth below. Your uses of such features constitute your agreement to be bound by these additional terms and conditions. These third-party terms are subject to change at such third party's discretion.

17.2. The Company is not responsible and does not assume any liability whatsoever for acts, errors or omissions of any third-party service provider.

18. Risk warnings

18.1. Trading of goods, real or virtual, which include virtual currencies (cryptocurrencies), involves a significant level of risk. Prices can fluctuate on any given day. Because of such price fluctuations, you may gain or lose value of your assets any moment. Currency may be subject to large swings in value and may even become worthless. You should carefully consider whether such trading is suitable for you in light of your circumstances and financial resources. We have highlighted some of those risks below:

- Traders put their trust in a digital, decentralized and partially anonymous system that relies on peer-to-peer (network in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system) networking and cryptography to maintain its integrity. This means that there is no central bank that can take corrective measures to protect the value of cryptocurrency in a crisis or issue more currency.
- Cryptocurrency trading is probably susceptible to irrational (or rational)

bubbles or loss of confidence, which could collapse in demand relative to supply. For example, due to the fundamentals of the cryptocurrency trading system's functioning, it is vulnerable to fluctuations in the level of confidence of market participants, which directly affects the level of demand or supply. The level of confidence can be affected both by purely economic factors and non-economic, including technological ones.

- Cryptocurrency transactions are irreversible. If you send cryptocurrency to an incorrect address, or send the wrong amount, you cannot get it back. We will not be liable for executing a transaction if the instruction relates to an incorrect address.
- Our website may suffer the failure of hardware, software, and Internet connections which may lead to communication failures, disruptions, errors, distortions or delays in payments and trading. You acknowledge that we will not be responsible for that.
- Any opinions, news, research, analyses, prices, or other information contained on Website are provided as general market commentary, and do not constitute investment advice.

There may be additional risks that we have not foreseen or identified in our Terms of Use.

Before buying or selling cryptocurrency, you should educate yourself about digital currencies. Buying and selling entails risks and could result in a complete loss of your funds. You should carefully overthink whether your financial situation and tolerance for risk is suitable for buying, selling or trading cryptocurrency. In case of bankruptcy or liquidation, the Company reserves the right not to return assets served as collateral for crypto loans or used to generate income or served.

19. Market volatility

19.1. Particularly during periods of high volume, illiquidity, fast movement or volatility in the marketplace for any digital assets or legal tender, the actual market rate at which a market order or trade is executed may be different from the prevailing rate indicated via the Services at the time of your order or trade. You understand that we are not liable for any such price fluctuations. In the event of a market disruption or Force Majeure event, we may do one or more of the following: (a) suspend access to the Services; or (b) prevent you from completing any actions via the Services, including closing any open positions. Following any such event, when trading resumes, you acknowledge that prevailing market rates may differ significantly from the rates available prior to such event.

20. Acceptable use

20.1. When accessing or using the Services, you agree that you will not violate any law, contract, intellectual property or other third-party right or commit a tort, and that you are solely responsible for your conduct while using our Services. Without limiting the generality of the foregoing, you agree that you will not: Use our Services in any manner that could interfere with, disrupt, negatively affect or inhibit other users from fully enjoying our Services, or that could damage, disable, overburden or impair the functioning of our Services in any manner; Use our Services to pay for, support or otherwise engage in any illegal gambling activities; fraud; money-laundering; or terrorist activities; or other illegal activities; Use any robot, spider, crawler, scraper or other automated means or interface not provided by us to access our Services or to extract data; Use or attempt to use another user's account without authorization; Attempt to circumvent any content filtering techniques we employ, or attempt to access any service or area of our Services that you are not authorized to access; Develop any third-party applications that interact with our Services without our prior written consent; Provide false, inaccurate, or misleading information; and Encourage or induce any third party to engage in any of the activities prohibited under this Section.

21. Disclaimer of Warranties

You understand that we cannot and do not guarantee or warrant that files available for downloading from the internet or the Websites will be free of viruses or other destructive code. You are responsible for implementing sufficient procedures and checkpoints to satisfy your particular requirements for anti-virus protection and accuracy of data input and output, and for maintaining a means external to our site for any reconstruction of any lost data.

WE WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY A DISTRIBUTED DENIAL-OF-SERVICE ATTACK, VIRUSES OR OTHER TECHNOLOGICALLY HARMFUL MATERIAL THAT MAY INFECT YOUR COMPUTER EQUIPMENT, COMPUTER PROGRAMS, DATA OR OTHER PROPRIETARY MATERIAL DUE TO YOUR USE OF THE WEBSITE OR ANY SERVICES OR ITEMS OBTAINED THROUGH ANY OF THE WEBSITES OR TO YOUR DOWNLOADING OF ANY MATERIAL POSTED ON IT, OR ON ANY WEBSITES LINKED TO IT. YOUR USE OF ANY OF THE WEBSITES, THEIR CONTENT AND ANY SERVICES OR ITEMS OBTAINED THROUGH THE WEBSITES IS AT YOUR OWN RISK. THE WEBSITE, ITS CONTENT AND ANY SERVICES OR ITEMS OBTAINED THROUGH THE WEBSITES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT ANY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. NEITHER THE COMPANY NOR ANY PERSON ASSOCIATED WITH THE COMPANY MAKES ANY WARRANTY OR REPRESENTATION WITH RESPECT TO THE COMPLETENESS, SECURITY, RELIABILITY, QUALITY, ACCURACY OR AVAILABILITY OF THE WEBSITES. WITHOUT LIMITING THE FOREGOING, NEITHER THE COMPANY NOR ANYONE RELATED TO OR ASSOCIATED WITH THE COMPANY REPRESENTS OR WARRANTS THAT ANY ONE OF OUR WEBSITES, ITS CONTENT OR ANY SERVICES OR ITEMS OBTAINED THROUGH THE WEBSITE WILL BE ACCURATE, RELIABLE, ERROR-FREE OR UNINTERRUPTED, THAT DEFECTS WILL BE CORRECTED, THAT OUR SITE OR THE SERVER THAT MAKES IT AVAILABLE ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THAT SUCH WEBSITE OR ANY SERVICES OR ITEMS OBTAINED THROUGH SUCH WEBSITE WILL OTHERWISE MEET YOUR NEEDS OR EXPECTATIONS.

THE COMPANY HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR PARTICULAR PURPOSE.

SOME JURISDICTIONS DO NOT ALLOW EXCLUSION OF WARRANTIES OR LIMITATIONS ON THE DURATION OF IMPLIED WARRANTIES, SO THE ABOVE DISCLAIMERS MAY NOT APPLY TO YOU IN THEIR ENTIRETY, BUT WILL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

22. Limitation on Liability

IN NO EVENT WILL THE COMPANY, ITS AFFILIATES OR THEIR LICENSORS, SERVICE PROVIDERS, EMPLOYEES, AGENTS, OFFICERS OR DIRECTORS BE LIABLE FOR DAMAGES OF ANY KIND, UNDER ANY LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH YOUR USE, OR INABILITY TO USE, ANY OF OUR WEBSITES, OR ANY WEBSITES LINKED TO THEM, ANY CONTENT ON THE WEBSITES OR SUCH OTHER WEBSITES OR ANY SERVICES OR ITEMS OBTAINED THROUGH OUR WEBSITE OR SUCH OTHER WEBSITES, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO, PERSONAL INJURY, PAIN AND SUFFERING, EMOTIONAL DISTRESS, LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS OR ANTICIPATED SAVINGS, LOSS OF USE, LOSS OF GOODWILL, LOSS OF DATA, AND WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), BREACH OF CONTRACT OR OTHERWISE, EVEN IF FORESEEABLE. THE FOREGOING DOES NOT AFFECT ANY LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW (WHICH MAY INCLUDE FRAUD).

THE COMPANY WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE ARISING FROM ANY USE OF YOUR ACCOUNT BY YOU OR BY ANY THIRD PARTY (WHETHER OR NOT AUTHORIZED BY YOU) INCLUDING BUT NOT LIMITED TO CYBER ATTACKS, UNAUTHORIZED ACCESS BY ANY THIRD PARTY.

23. Indemnification

You agree to defend, indemnify and hold harmless the Company, its affiliates, licensors and service providers, and its and their respective officers, directors, employees, contractors, agents, licensors, suppliers, successors and assigns from and against any claims, liabilities, damages, judgments, awards, losses, costs, expenses or fees (including reasonable attorneys' fees) arising out of or relating to your violation of these Terms of Use or your use of any Websites or any Services, including, but not limited to, any use of any Website's content, services and Services other than as expressly authorized in these Terms of Use or your use of any information obtained from any of the Websites.

24. Feedback and Comments

24.1. If you have any feedback, comments, requests for technical support, or other communications relating to the Website, you may contact support by e-mail: support@rival.finance.

25. Governing Law and Jurisdiction

25.1. All matters relating to the Websites or any particular Services and these Terms of Use and any dispute or claim arising therefrom or related thereto (in each case, including non-contractual disputes or claims), shall be governed by and construed in accordance with the internal laws of Republic of Lithuania without giving effect to any choice or conflict of law provision or rule (whether of Republic of Lithuania or any other jurisdiction).

25.2. Any legal suit, action, or proceeding arising out of, or related to, these Terms of Use or the Website or any Services shall be instituted exclusively in the courts of the Republic of Lithuania although we retain the right to bring any suit, action or proceeding against you for breach of these Terms of Use in your country of residence or any other relevant country.

26. Waiver and Severability

26.1. No waiver of the Company of any term or condition set forth in these Terms of Use shall be deemed a further or continuing waiver of such term or condition or a waiver of any other term or condition, and any failure of the Company to assert a right or provision under these Terms of Use shall not constitute a waiver of such right or provision.

26.2. If any provision of these Terms of Use is held by a court or other tribunal of competent jurisdiction to be invalid, illegal or unenforceable for any reason, such provision shall be eliminated or limited to the minimum extent such that the remaining provisions of the Terms of Use will continue in full force and effect.

27. Entire Agreement

27.1. The Terms of Use, and any other terms and policies constitute the sole and entire agreement between you and us with respect to the Websites and supersede all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, with respect to the Websites.

28. Complaints

28.1. If you have a complaint, you can submit a complaint using our online form or contact the team at support@rival.finance. Once we have received your complaint, we will acknowledge this via email. We will then investigate all the details of your complaints, and issue our response within a couple of business days, but this can take up to 15 business days.

Annex to Walletto General Terms and Conditions

PROHIBITED ACTIVITY LIST

When using the Walletto Services, you are prohibited from receiving or making payments in connection with the following activities:

1. Illegal gambling services (including, but not limited to, illegal online casinos, sports betting, betting, reverse auctions and lotteries);
2. Quick enrichment schemes, Ponzi schemes, snowball schemes, investment clubs or similar activities;
3. Adult or sexual content, escort services or modeling agencies;
4. Mass email services, SMS services or customer marketing lists;
5. Prescription drugs, prohibited substances or components thereof; drug paraphernalia;
6. Counterfeit or forged goods, novelty ID;
7. Dangerous or restricted goods (including but not limited to explosives, radioactive materials, toxic substances, batteries, fireworks);
8. Weapons, knives and ammunition;
9. Protected works of art, history and culture;
10. Restricted electronics (eg, cable television decoders, radars, and surveillance equipment);
11. any other goods or services the sale, supply, delivery, offer or marketing of which is prohibited or restricted in the jurisdiction of the Seller or in any jurisdiction in which any of its customers is located.

We may change or extend the list of prohibited goods or services at any time by notifying you. If you supply goods or services that are subject to a subsequent extension of the list, you shall immediately cease to make payments for such goods or services.

In the event that you fail to comply with such termination, we reserve the right to terminate the business relationship and the validity of the Walletto General Terms and Conditions. If you are in doubt as to whether your goods or services fall into any of the categories listed, you should first consult us before offering such goods or services.

WALLETTO GENERAL TERMS AND CONDITIONS

1. General Provisions

1.1. These Walletto General Terms and Conditions establishes relationship between Walletto and the Client and set out rights, obligations and other terms when the Client opens, uses and closes the Payment Account and uses other services provided by Walletto.

1.2. Before using the Walletto Services, the Client must read these Walletto General Terms and Conditions.

1.3. The Walletto General Terms and Conditions enters into force and is valid indefinitely when the Client registers in the System, has read the General Terms and Condition and expresses consent to comply with them.

1.4. We provide the following services in accordance with these Walletto General Terms and Conditions, unless we and you agree otherwise:
1.4.1. issuing and redemption of electronic money;
1.4.2. services enabling cash to be placed on an Account as well as all the transactions required for operating an Account;
1.4.3. services enabling cash withdrawals from an Account as well as all the transactions required for operating a payment account;
1.4.4. execution of the following types of Payment transactions:
1.4.4.1. direct debit, including one-time direct debit;
1.4.4.2. payment transactions using a payment card or similar device; and
1.4.4.3. credit transfers, including standing orders.
1.4.5. issuing payment instruments or accepting payment transactions; 1.4.6. money remittance.

1.4. The terms and conditions of other services provided by us are set out in the appendices to these Walletto General Terms and Conditions and in the separate agreements that are an integral part of the Walletto General Terms and Conditions. The terms and conditions set out in the Annexes are special provisions that go beyond the other provisions of the Walletto General Terms and Conditions.

2. Definitions

2.1. **Account** - the account opened in our System for your use;

2.2. **Business Day** - any day other than a Saturday or a Sunday or a public or bank holiday in Lithuania;

2.3. **Cardholder** - an individual to whom the card is issued to and who is authorized to use the card;

2.4. **Commission fee** means the fee charged by us for a payment operation and/ or related services.

2.5. **Consumer** means the natural person who operates under these Walletto General Terms and Conditions and its annexes and does not pursue aims which are not consistent with business, commercial or professional activity of this person;

2.6. **Confidential Information** means any information which is marked as “Confidential” or “Proprietary” or should be reasonably expected to be confidential having regard to the context of disclosure or the nature of the information; including, without prejudice to the generality of the foregoing, the terms of these Walletto General Terms and Conditions as well as business plans, data, strategies, methods, client and client lists, technical specifications, transaction data and customer data shall be deemed confidential;

2.7. **Client**, **you** or **your** means the natural person or legal entity accepting these Walletto General Terms and Conditions;

2.8. **Electronic money** means electronically, including magnetically, stored monetary value as represented by a claim on the issuer (us) which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer. For the ease of reference in these Walletto General Terms and Conditions when referring to electronic money stored on your account we will use the term ‘**Funds**’;

2.9. **Payer** means a natural or legal person submitting a payment order;

2.10. **Security Credentials** means any personalized features that you create or receive and use for access to the Account or initiation and management of separate Services provided by us and/or initiation, authorization, implementation, confirmation and reception of payment operations;

2.11. **Payment Instrument** means a personalized tool and / or certain procedures agreed between us and you which are used by you for the initiation of the Payment order.

2.12. **Payment transfer** means a payment service when money is transferred to your Account under the initiative of the Payer;

2.13. **Payment order** means an order from the Payer or the Recipient (payment transfer) for the provider of payment services to execute a payment operation;

2.14. **Payment operation** means a money deposit, transfer or withdrawal initiated by the Payer or the Recipient;

2.15. **Payment transaction** means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

2.16. **Prices** means the prices for our services and operations confirmed in accordance with the procedure established by us;

2.17. **Recipient** means a natural (private) or legal person indicated in the Payment order as a Recipient of the payment;

2.18. **Services** means payment and e-money services identified in the clause 1.4 of these Walletto General Terms and Conditions and provided by us;

2.19. **System**, **we**, **our**, or **us** means Walletto;

2.20. **A unique identifier** is a combination of letters, numbers and symbols that we, as a payment service provider, provide to you and is used to identify the payment services involved in the Payment transaction and / or your Account used in the Payment transaction.

2.21. **Walletto** – is UAB "Walletto", company code 304686884, registered office: Žalgirio str. 92-805, 09303 Vilnius, Lithuania, email: info@walletto.eu, website address: www.walletto.eu. Walletto is registered in the Register of Legal Entities of the Republic of Lithuania and owns an electronic money institutions license No 33, issued by the Bank of Lithuania on 29 March 2018. The Bank of Lithuanian supervises Walletto. You can find more information about the supervisory authority by clicking this link https://www.lb.lt/en/.

3. Registration in the System

3.1. To start using our services, you must first submit an application to open an account and provide the information and documents we request for the Account to legal persons and natural persons.

3.2. The Account of a natural person cannot be used for income received from a business relationship unless there are appropriate supporting documents (business certificate, certificate of individual activity, etc.). If the Client violates this clause, Walletto has the right to close the Account.

3.3. In the event of a higher risk, the client must provide additional documentation to meet the requirements for enhanced customer identification. During this waiting period, we have the right to suspend the use of the Account and if the client does not respond within 45 (forty five) days of such request, we have the right to terminate the business relationship.

3.4. We reserve the right to refuse to register you as a new client without giving any reason, but we guarantee that refusal to register will always be based on important reasons that we do not have to or have no right to disclose.

3.5. You are solely responsible for providing the information and documents we request. You are responsible for ensuring that all information provided during or at any time after the registration process is accurate and correct.

3.6. We reserve the right to refuse your right to use the Services if you do not provide the information and documents requested or provide inappropriate documents. We are not obligated to provide the Services to the requesting client and may, in our sole discretion, reject an application for the Services.
3.7. After we have verified the documents and information provided by you, you have the right to start using Account and our Service

3.8. You have the right to open one account unless we expressly approve the opening of any additional accounts.

3.9. If your account has not been used for more than 12 months and there are no funds in it, inform you about it and without receiving your answer, we reserve the right to close it automatically.

3.10. If you have not used your Account for more than 12 months (there are no transactions on it) but it has funds in it and after our report, you do not withdraw the money, we have the right to charge an inactive account administration fee (published in the Price list). This fee is used to cover the administration costs of an unused Account until the Account balance becomes empty and is automatically closed. You will be informed in advance to your email address.

4. Issuance and redemption of Electronic money

4.1. Your Account allows you to deposit, transfer, hold funds in the Account for transfers, execution of local and international money transfers, payment of contributions, as well as to receive money in the Account, pay for goods and services and perform other operations directly related to money transfers. You may use all of our services only if you have completed identification procedures in accordance with the rules set forth in our System.

4.2. Funds in your Account are considered electronic money that we issue after you transfer or deposit money to your Account. When you deposit or transfer money to your Account and we receive money, we credit it to your Account, at the same time issuing Electronic Money at face value. Electronic money is credited and stored in your Account.

4.3. You choose the specific method of depositing or transferring funds to your Account by selecting a certain method/function in the Account, which provides instructions on how to deposit money for each payment instrument.

4.4. The nominal value of electronic money corresponds to the value of the money deposited or transferred to your Account (after deducting the standard commission fee applicable to a specific payment instrument).

4.5. The electronic money held in your Account is not a deposit and under no circumstances do we pay any interest on the electronic money held in your Account and do not provide any other benefits related to the Electronic money storage period.

4.6. At your request, electronic money held in your Account will be redeemed at their nominal value at any time, unless we and you agree otherwise.

4.7. You submit a request for redemption of Electronic money by generating a Payment order to transfer Electronic money from your Account to any other account specified by you.
4.8. No special conditions for the redemption of Electronic money that differ from the standard conditions for transfers made in your Account and other Payment transactions apply. You choose the amount of Electronic money to be redeemed or transferred.

4.9. There is no additional charge for redeeming Electronic Money. When redeeming Electronic Money, you pay a standard Commission fee for the transfer or withdrawal of money, which depends on the method of transfer or withdrawal of Electronic Money you have chosen. Standard fees apply for money transfers or withdrawals.

4.10. Funds in your Account are protected in accordance with the requirements of legal acts by separating them from own Walletto funds and are kept in a separate account with a credit institution in Lithuania or one of the Member States of the European Union.

4.11. Provided that you terminate these Walletto General Terms and Conditions and apply with the request to close your Account and delete your Account from our System, or we terminate the provision of our Services to you and delete your Account from our System in cases provided in these Walletto General Terms and Conditions, money held on your Account shall be transferred to your bank account or to the account in another electronic payment system indicated by you. We have the right to deduct from the repaid money the amounts that belong to us (prices for Services provided by us and expenses which have not been paid by you, including but not limited to, fines and damages incurred by us due to a breach of these Walletto General Terms and Conditions committed by you, which have been imposed by financial institutions and (or) other competent authority of state). In the event of a dispute between us and you, we have the right to detain money under dispute until the dispute is resolved.

4.12. In case we fail to repay the money to you due to reasons beyond the control of us, you shall be notified thereof immediately. You shall immediately indicate another account or provide additional information necessary to repay the money.

5. **Authorisation of Payment transactions**

5.1. A payment transaction shall be considered to be authorised only when the Payer has given consent to execute the Payment transaction. In the absence of consent, the Payment transaction shall be considered to be unauthorised.

5.2. The consent may be provided to us in the form and manner agreed between us and you. In case if the consent is provided in written, it shall be signed properly. The consent may be confirmed by using the security code given to you by us and login credentials during the time of the creation of the Account or by other identity verification means. The consent may be expressed by other form and manner needed for the concrete Services and / or indicated in the additional agreement between us and you.

5.3. You are obligated to check the information about the executed Payment transactions at least 1 (one) time per month.

5.4. You are obligated to inform us in writing about the unauthorised or improperly executed Payment operations, including the noticed mistakes, inaccuracies in the statement without undue delay from the acknowledging of such circumstances and in any case not later than within 13 (thirteen) months after the debit date. The other terms of informing us about the circumstances described above may be used in cases set forth by the additional agreements signed between the Parties.

5.5. In case you do not notify us about the circumstances described in the clause 5.5 of these Walletto General Terms and Conditions within the terms indicated in these Walletto General Terms and Conditions and the additional agreements between the Parties, Walletto has no obligation to return the amount of the unauthorised Payment transaction.

5.6. If the Client denies the authorisation of the executed Payment transaction or the payment transaction were executed improperly, we are obligated to prove that the

Payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency in the Services provided by us.

5.7. The use of the means of identification and access to the Account credentials is the sufficient proof, that the Client authorised the Payment transaction or acted fraudulently or failed with intent or gross negligence to fulfill one or more of his obligations set forth in the clauses 13.1 – 13.6 of these Walletto General Terms and Conditions.

5.8. In accordance to the terms indicated in the clause 5.5 of these Walletto General Terms and Conditions or having determined that the Payment operation was not authorised by the Client, we without undue delay, but no later than by the end of the next Business day, return the amount of the unauthorised Payment transaction to the Client and, where applicable, - restore the balance of the Account from which this amount was written down and which would have existed if the unauthorised Payment transaction had not been executed, unless we have reasonable grounds to suspect fraud and inform the supervisory authority in writing of those reasons.

5.9. The Client may incur all the losses of up to 50 (fifty) Euros resulting from unauthorised payment transactions if these loses have been incurred due to:
5.9.1. use of a lost or stolen payment instrument, if the authorisation happened before client has notified Walletto of the loss or theft of payment instrument; 5.9.2. illegal acquisition of a payment instrument if the Client had not protected personalized security features (including identity verification instruments).

5.10. The Client shall be liable for any losses caused by unauthorised Payment transaction, if the Client incurred them by acting fraudulently or by failing to fulfil, with gross negligence or intent, one or more of his obligations set forth in the clauses 13.1-13.6 of these Walletto General Terms and Conditions and additional agreements signed by the Parties.

5.11. Other terms of the liability of the Parties for the unauthorized Payment operations may be indicated in the additional agreements between the Parties.

6. Execution and cancellation of Payment orders

6.1. The Payment order shall be considered received by us (the execution period of such Payment order shall start to run) on the day of its receipt or, if the Payment order is not received on our business day, the Payment order shall be considered received on the next business day. If for the execution of the Payment transaction we require you to provide supporting documents, the Payment order shall be considered to be received by us on the day when you submit the requested documents.

6.2. The Payment order we received on a Business day, but not during our business hours, is considered to be received on the next Business day.

6.3. Payment orders in our System are executed immediately (up to a few minutes, unless the Payment transaction is suspended due to the cases provided for in the legislation and these Walletto General Terms and Conditions), regardless of our business hours.

6.4. We execute Payment transactions according to the Unique identifier provided in the Payment Order - IBAN Account number.

6.5. We are not liable if the Payment order does not contain a unique identifier and / or is incorrect and / or the Beneficiary's payment service provider has set another unique identifier for the proper execution of such Payment transaction (including funds in the Beneficiary's payment account).

6.6. We have the right to request additional and / or other mandatory information (such as amount and currency, Beneficiary's name, surname / legal entity name / payment code) that must be provided to us in the Payment order for the purpose of proper execution of the Payment transaction.

6.7. Prior to the execution of a Payment order, we undertake to provide you with information on the possible maximum deadlines for the execution of a particular Payment order, the Commissions payable and how they are distributed. You can find this information on our website and in your personal Account.

6.8. The procedure of cancellation of the Payment order:
6.8.1. the Payment order cannot be canceled after we receive it, except for cases provided in these Walletto General Terms and Conditions;
6.8.2. if the Payment operation had been initiated by the Recipient, the Payer cannot cancel the Payment order after the Payment order has been sent or the Payer has given the consent to the Recipient to perform the Payment operation;
6.8.3. the Payment order may be canceled only if the Client (Payer) and we agree on it, but the consent of the Beneficiary is required.

6.9. We have the right to record and store any Payment orders submitted in a manner agreed with us, as well as to record and store information about all Payment transactions performed by you or in accordance with your Payment orders. We may provide the above-mentioned records to you and / or third parties who, on the grounds established by law, have the right to receive such data as proof confirming the submission of Payment orders and / or performed Payment transactions.

6.10. We have the right to refuse to execute a Payment order if there are reasonable doubts that the Payment order was submitted by you or your authorized representative, the Payment order or the submitted documents are legal. In such cases, we have the right to require you to additionally confirm the submitted Payment order and / or submit
documents confirming the right of persons to manage the funds in the Account or other documents specified by us in a manner acceptable to us by e-mail at your costs. We will not be liable for any losses that may result from the refusal to execute the submitted Payment order due to your refusal to provide additional information or documents.

6.11. You are responsible for ensuring that there is sufficient money in your Account in the relevant currency to execute the Payment order.

6.12. We have the right to use third parties to partially or fully execute your Payment order if your interests and / or the essence of the Payment order so require. In the event that the essence of your Payment order requires that the Payment transaction be further sent and executed by another financial institution, but this institution suspends the Payment order, we are not responsible for such actions of that financial institution, but we try to find out the

reasons for the Payment order suspension.

6.13. We have the right to suspend and / or terminate the execution of your Payment Order if required by law or for other reasons beyond our control.

6.14. If we refuse to execute your Payment order, we will promptly notify you or provide you with the necessary conditions to access such notice, unless such notice is technically impossible or prohibited by law.

6.15. We do not accept or execute your Payment orders in order to carry out transactions on your Account if the funds in the Account are seized, your right to manage the funds is otherwise restricted by law or the transactions are suspended in accordance with applicable law.

6.16. If the money transferred by the Payment order is returned due to reasons beyond our control (inaccurate data of the Payment order, the Beneficiary's account is closed, etc.), the refunded amount will be credited to your Account. The commission fees paid by the Payer for the execution of the Payment order shall not be refunded, and other fees related to the refund and applicable to us may be deducted from your Account.

6.17. The terms and conditions for the execution of Payment transactions and the duration of the execution of other Services are set out in these Walletto General Terms and Conditions, the Price List and other additional agreements between us and you.

6.18. When you are a Payer and the Payment transaction is performed in euros in the Republic of Lithuania and other Member States, we ensure that the amount of the Payment transaction is credited to the Beneficiary's account on the day of the Payment transaction, if the execution date of the Payment order is not our Business day, it is the next Business day. When you are a Payer and a Payment transaction is made in the currencies of non-euro area Member States in the Republic of Lithuania and other Member States, we ensure that the Payment transaction amount is credited to the Beneficiary's account on the day of the Payment transaction, and, if the Payment order execution date is not our Business day, then the nearest Business Day for Payment transactions, but not later than within 3 (three) Business days after we have received the Payment order.

6.19. The maximum limits for the costs of Payment transactions executed by the Payment instrument may be specified in additional agreements signed between us and you.

6.20. We may provide you with an Account statement for your Payment transactions, which could be can be submitted through your Account, including the following information:
6.20.1. amount of the Payment transaction in the currency specified in the Payment order;
6.20.2. commissions paid for Payment transactions and how they are distributed; 6.20.3. the valid exchange rate and the amount of the Payment transaction after the exchange rate, if the currency was exchanged during the Payment transactions; 6.20.4. date of debiting from the Account;
6.20.5. date of income to the Account;
6.20.6. other information that will be provided to you in accordance with the applicable legal acts of the Republic of Lithuania.

7. Account blocking

7.1. The Account may be blocked by the Client's initiative and / or the Account (including the payment instrument if such is given to the Client) may be blocked if the Client submits a respective request to us. We have the right to demand that the request submitted by the Client's oral request to block the Account (including the payment instrument if such is given to the Client) be subsequently approved in writing or in another manner acceptable to us.

7.2. If we have the reasonable doubts that the request indicated in the clause 7.1 of these Walletto General Terms and Conditions is not submitted by the Client, we have the right to refuse to block the Account (including the payment instrument if such is given to the Client). In such cases, we shall not be liable for any losses that may result from the failure to comply with the said request.

7.3. We have the right to block the Account (suspend the execution of Payment transactions in whole or in part, and limit the crediting of funds to the account) and / or the Payment instrument, if such instrument has been provided to you:
7.3.1. if there are objectively justified reasons related to the security of the funds and / or Payment instrument in the Account, the alleged illegal or unfair use of the funds and / or payment instrument in the Account;
7.3.2. in the event that you do not comply with the terms of these Walletto General Terms and Conditions;
7.3.3. in the event that we have reasonable suspicions that the funds in the Account may be used for illegal activities, including, but not limited to, the performance of criminal activities ;
7.3.4. on other grounds established by the legal acts of the Republic of Lithuania and / or in the cases specified in the additional agreements signed by the Parties.

7.4. We undertake to inform you about your suspected or actual fraud or threat to the security of the Services in your personal Account by telephone or e-mail, by post or any other means which is secure and appropriate at the time .

8. Prices for Services (Commission fee and currency exchange)

8.1. The prices of our Services are listed in the Annex "Price List", which is an integral part of these Walletto General Terms and Conditions. Prices for Services are also listed on our website at https://walletto.eu/price-list/.

8.2. Our standard Services are charged in accordance with these Walletto General Terms and Conditions and the Price List. Services that are not defined here and / or in the Price list will be charged at individual prices that you will be notified of before using such services.

8.3. You pay us a commission for the payment services and / or related services we provide. The commission fee is specified in the Price List and / or in the additional agreement signed with you.

8.4. All Prices and Commissions payable by you will be deducted from your Account balance. If your Account balance is insufficient or your Account balance becomes negative, we reserve the right to bill you for any deficiencies/shortfall.

8.5. If we do not have the possibility to deduct the Prices and / or Commission fee payable for the Services provided from the balance of your Account, we will issue a separate

invoice for the amount of the debt. Invoices shall be paid within 10 (ten) days from the date of issue of the invoice. In the event of late payment, we reserve the right to charge 0.02 % interest and / or terminate this Walletto General Terms and Conditions immediately upon written notice to you.

8.6. In the event that there are insufficient funds in your Account to execute the Payment transaction and pay the Commission Fee, we have the right to refuse to execute the Payment transaction.

8.7. Unless otherwise stated, prices and commissions are in Euros.

8.8. Exchange rates will be provided to you prior to the Payment order.

8.9. Currency exchange is based on the exchange rate of European Central Bank (https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/index.en.html) and are valid at the time of conversion.

8.10. We may apply the changed base exchange rate immediately without notice.

8.11. In the event that the currency in which the Payment transaction is made is different from the currency in which the Account is debited, the conversion of such currencies shall be carried out in accordance with European Central Bank rate effective at the time of transaction. The ECB rates are published on https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/index.en.html.

9. Communication

9.1. These Walletto General Terms and Conditions, all communications, information about any changes to the Services and the Price Information are in English. You acknowledge that all communication between us and you will be in English.

9.2. Information is provided to you in the following ways:
9.2.1. the information may be provided in person, through Your Account, sent by mail, e-mail, telephone and other means of telecommunications, including electronic means;
9.2.2. the information may be published on our website, and we may also provide the information in the press or other media. It is considered that the information provided to the public has been duly communicated to you, except in cases of mandatory requirements of the laws and other legal acts of the Republic of Lithuania and / or cases where we are obliged to inform you personally.

9.3. You acknowledge that any communication between us and you will primarily take place through the Account and email. Disclosure of any information in our account and email means that the information provided is relevant and effective.

9.4. You acknowledge that communication through the Account will only take place if you enter in your personal account the login details or other requested personal security credentials we have provided to you for the purpose of authenticating you as a Client.

9.5. Possible communication by e-mail is performed between our e-mail specified on the

website and your e-mail that you provided during registration. E-mail message is considered to be duly delivered on the following Business Day.

9.6. If you communicate by phone, you will be verified based on your data. Telephone communication between us and you is possible during our working hours. The message is considered to have been properly transmitted by telephone at the time of the conversation with you.

9.7. When communicating by mail, letters are delivered to the other party's address. The letter will be considered to have been duly served on the third day after sending out, even if notification that the letter cannot be served to the other party or that the other party has rejected the letter or has not withdrawn it within the prescribed time limit, even if the addressee was unaware of the letter.

9.8. Information published on our website, in your Account, as well as publicly disclosed information is deemed to have been properly served on the date of publication / publication of such information.

9.9. You agree that we may record, even without notice, any ongoing communication between us and you, using any technical means available, and archive all records, as well as copies of any information and documents we receive from you and third parties. You agree that we may use this information at any time for the purposes set out in these Walletto General Terms and Conditions or to ensure that these Walletto General Terms and Conditions are complied with.

9.10. You have the right to receive information about these Walletto General Terms and Conditions and these Walletto General Terms and Conditions in paper form or on any other durable medium on which we may provide such information.

10. Prohibited activities

10.1. When using the Walletto Services, you are prohibited from receiving or making payments in connection with the activities covered under our Prohibited Activity List available on our website and as Annex 1 to these Walletto General Terms and Conditions.

10.2. We may change or extend the list of prohibited goods or services referred to in clause 10.1 at any time by notifying you. If you supply goods or services that are subject to a subsequent extension of the list referred to in clause 10.1, you shall immediately cease to make payments for such goods or services. In the event that you fail to comply with such termination, we reserve the right to terminate the business relationship and the validity of these Walletto General Terms and Conditions. If you are in doubt as to whether your goods or services fall into any of the categories listed, you should first consult us before offering such goods or services.

11. Changes to these Walletto General Terms and Conditions and Prices

11.1. These Walletto General Terms and Conditions may be amended from time to time.

11.2. We reserve the right to unilaterally change these Walletto General Terms and Conditions, applicable Prices and Commissions and / or Terms of Service.

11.3. We undertake to inform you at least 60 (sixty) calendar days in advance of any

changes to these Walletto General Terms and Conditions, applicable Prices and Commission Fees and / or Terms of Service that aggravate your situation (e.g. increase existing Prices).

11.4. We will personally notify you of any changes in the applicable Prices and Commissions and / or Terms of Service by the means specified in Section 9 of these Walletto General Terms and Conditions.

11.5. If you do not agree to the proposed changes, you have the right to terminate these Terms and Conditions immediately and free of charge before they take effect.

11.6. We have the right to change these Walletto General Terms and Conditions, the applicable Prices and Fees and / or the Terms and Conditions of the Service for important reasons and without notifying the terms specified in Clause 11.3 of these Walletto General Terms and Conditions. In such cases, we will immediately notify you of any changes to the Service by posting the information on our website and / or by e-mail and / or electronic mail. In this case, you have the right to terminate these Walletto General Terms and Conditions immediately by notifying us in writing or in any other manner agreed between us and you of the termination of these Walletto General Terms and Conditions.

11.7. Termination of these Walletto General Terms and Conditions in accordance with clauses 11.6 or 11.7 does not release you from our obligations arising before the date of termination of these Walletto General Terms and Conditions for their proper performance.

11.8. If you do not use your right to terminate these Walletto General Terms and Conditions in accordance with the clauses 11.5 or 11.6 of these Walletto General Terms and Conditions, you shall be deemed as accepted the changes to these Walletto General Terms and Conditions, applicable Prices and Commission fees and / or the terms of Services made. If you agree with the changes to these Walletto General Terms and Conditions, applicable Prices and Commission fees
and / or the terms of Services, then you are not entitled subsequently to submit to us your objection and / or claims regarding the content of such changes.

12. Validity and termination

12.1. You have the right to terminate this Agreement by notifying us in writing 30 (thirty) days in advance. You may also terminate this Agreement free of charge at any time before the proposed effective date of the amendments to these Walletto General Terms and Conditions in accordance with the terms and conditions set forth in Section 9 of these Walletto General Terms and Conditions.

12.2. We reserve the right to terminate these Walletto General Terms and Conditions from the date of notice to you if:
12.2.1. you file a petition for bankruptcy, become insolvent, or make any arrangement or composition with or assignment for the benefit of its creditors, or a receiver is appointed for you or your business, or you into liquidation either voluntarily (otherwise than for reconstruction or amalgamation) or compulsorily;
12.2.2. You violate these Walletto General Terms and Conditions or act in violation of these Walletto General Terms and Conditions and do not provide remedies within the time period specified by us; 12.2.3. we have reasonable grounds to suspect that you or a person authorized to act on your behalf are acting in a manner inconsistent with generally

binding legal requirements, good morals, fair dealing, anti-money laundering conditions, or that your circumstances have changed materially to ensure compliance with these Walletto General Terms and Conditions; 12.2.4. you have outstanding obligations to us;
12.2.5. competent authorities (the police, Bank of Lithuania or others) instructs us to terminate a business relationship with you;
12.2.6. the information provided by you and used in these Walletto General Terms and Conditions appears to be false, incomplete, inaccurate and incomprehensible;
12.2.7. it has been proven that your fraudulent activities were related to the use of your Account or that you and / or your employees have been prosecuted for fraudulent activities;
12.2.8. if we continue to provide our services to you, we will violate the rules or recommendations of our bank or other partners.

12.3. For other reasons, we have the right to terminate these Walletto General Terms and Conditions and its supplements by giving you 60 days notice of termination.

12.4. Termination of these Walletto General Terms and Conditions shall not relieve the Parties of any obligations to each other arising prior to the date of termination of these Walletto General Terms and Conditions for the proper performance thereof.

13. Security requirements for the Account use

13.1. You are responsible for the safety of devices used to log in to the Account, shall not leave them unattended, in public places or otherwise easily accessible to third persons.

13.2. It is prohibited to connect to your account using the services of a layered router (TOR network), constantly connecting from an Internet Protocol (IP) address in different countries.

13.3. It is recommended to update software, applications, anti-virus programs, browsers and other programs in time.

13.4. It is recommended to protect devices with passwords, PIN codes or other safety instruments.

13.5. The Client undertakes to carefully evaluate incoming e-mails, even if Walletto is listed as the sender. Walletto never asks customers to download attachments or install software. Fraud e-mail attachments may contain viruses that could harm your device or compromise your Account.

13.6. It is recommended not to click on unknown links, open unknown documents, install software or application from unknown, unreliable sources or visit unsafe websites.

13.7. If you notice any suspicious activity on his account and think that third persons may have logged in to system for the using of the Services, you shall:
13.7.1. immediately inform us thereof and request to block your Account; 13.6.2. in order to continue to use the Account, you shall change the password, use other additional account confirmation instruments or use safer instruments and delete unsafe additional login confirmation instruments.

14. Liability of the Parties

14.1. Each Party is liable for all fines, forfeits, and other losses which the other Party incurs due to violation of the Agreement by the guilty Party. The guilty Party undertakes to reimburse direct damage incurred due to such liability to the affected Party.

14.2. If the Payment transaction is executed incorrectly, we will only be liable through our own fault. We are not responsible for the mistakes of third parties.

14.3. If you initiate a Payment order, the Payment order shall be executed by identifying the unique identifier, such Payment order shall be deemed duly executed if it has been executed in accordance with the specified unique identifier. We have the right, but not the obligation, to verify that the unique identifier provided in the Payment order we receive corresponds to the name and surname of the account holder.

14.4. If the unique identifier is presented to us with the Account to be credited or debited from the Account, the Payment order is deemed to be executed properly if it was executed according to the specified unique identifier. If we carry out the said inspection (for example, in the prevention of money laundering risk) and find out clear mismatch between the unique identifier submitted to us and the Account holder's name, we shall have the right not to execute such a Payment order.

14.5. We are responsible for a duly initiated Payment order in accordance with these Walletto General Terms and Conditions and / or additional agreements signed by the Parties.

14.6. If you (the Payer) properly initiate the Payment order and the Payment transaction is not executed or executed incorrectly, we will immediately and free of charge take steps to trace the Payment transaction and inform you about the search results.
14.7. We are responsible for non-application of the Commissions or non-refund of the already paid Commission fee in case the Payment order has not been executed or improperly executed due to our fault.

14.8. We are only liable for your direct losses related to a non-executed Payment order or an incorrectly executed Payment order.

14.9. We are not responsible for claims between the Beneficiary and the Payer and we do not deal with such claims. You can only make a claim against us for non-performance or improper performance of our obligations.

14.10. The limitations of our liability do not apply if such limitations are prohibited by applicable law.

14.11. The conditions for refunding the amount of Payment Transactions initiated by the Beneficiary or the Beneficiary shall be the same as those established in the Law on Payments of the Republic of Lithuania, unless the Parties have agreed otherwise.

15. *Force Majeure*

15.1. Under no circumstances shall a Party be liable for non-compliance with the Walletto General Terms and Conditions if the Party proves that the Contract has not been performed due to *force majeure* circumstances, which shall be proved in accordance with the procedure established by law. The Party shall notify the other Party in writing about the

circumstances of *force majeure* within 10 (ten) calendar days from the date of occurrence of such circumstances

15.2. Without limiting clause 15.1, we shall not be liable for any failure of any IT system, communication system or payment system, whether such failure is caused by a failure of hardware or software. This does not apply to failures of our systems or systems under our direct technical control and access if we have not complied with safeguards against their failures under the business continuity plan in accordance with common industry practice and have failed to reasonably mitigate the consequences of the failure.

16. Representation and Warranties

16.1. You represent and warrant that:
16.1.1. if you are a corporate entity, you are validly incorporated and lawfully exist under the laws of the jurisdiction of incorporation or any country or territory in which you conduct business;
16.1.2. your execution of and performance under these Walletto General Terms and Conditions in no way breaches, contravenes, violates or in any manner conflicts with any legal obligation including, without limitation, your corporate charter or similar document or any agreement between you and any third party or any affiliated entity;
16.1.3. you have obtained and will maintain all necessary consents, authorisations, permissions and other facilitating acts in order to lawfully perform your obligations under these Walletto General Terms and Conditions;
16.1.4. you may lawfully conduct your business in any country or territory into which you sell, provide, deliver, promote or market your goods or services that you have obtained all necessary authorisations, clearances, licences or consents to do so;
16.1.5. all information provided by you to us in connection with your Application and these Walletto General Terms and Conditions is and remains complete and accurate; 16.1.6. the person entering into these Walletto General Terms and Conditions on your behalf is duly authorised to do so;
16.1.7. you do not offer and do not intend to offer goods or services prohibited under section 10; and
16.1.8. you will always comply with your obligations under these Walletto General Terms and Conditions in accordance with applicable law.

17. Personal Data Protection

17.1. Each party, when acting as data controller (as defined in Regulation (EU) 2016/679 of the European Parliament and the Council, hereinafter the “Data Controller”), shall process personal data in accordance with applicable data protection laws.

17.2. Where one party acts as the data processor (as defined in the Regulation (EU) 2016/679 of the European Parliament and the Council, hereinafter the “Data Processor”) of personal data which is processed by the other party as the Data Controller, the Data Processor shall at all times follow the Data Controller’s reasonable instructions with regards to the personal data processed.

17.3. The processing of personal data, data subjects and their rights, conditions for the storage of personal data are defined in our Privacy Policy.

18. Confidentiality

18.1. During and after the validity of these Walletto General Terms and Conditions, each party will use and reproduce the confidential information of the other party only for the purposes of these Walletto General Terms and Conditions and only to the extent necessary for this purpose. Information to your employees, consultants or independent contractors on need to know basis can be provided only prior to signing non-disclosure consent.

18.2. Notwithstanding the foregoing, a party shall not be deemed to have breached the confidentiality provisions if required to do so by law or by order of a competent court or governmental authority.

18.3. No obligation of confidentiality shall apply to information which (i) is in the public domain or becomes public knowledge without the action of the other party; (ii) is known to the receiving Party without restriction before being received from another Party by its own independent sources as evidenced by written records of such Party and not directly or indirectly required by the other Party; (iii) is obtained by a party from any third party legally entitled to transmit such information, without any obligation to keep such information confidential; or (iv) is created independently by employees or agents of the receiving Party, provided that such Party can demonstrate that their employees or agents did not have access to the confidential information.

19. Applicable law and dispute settlement

19.1. These Walletto General Terms and Conditions are drawn up and interpreted in accordance with Lithuanian law. Lithuanian law applies to the conditions not covered by the Walletto General Terms and Conditions.

19.2. The disputes between you and us shall be solved through negotiations.

19.3. In the event that the dispute cannot be resolved through negotiations, you may file a complaint by mail or email, stating your name, contact details and relevant information showing why we have violated your legal rights and interests. You may add other available evidence to substantiate the need for such a complaint. To file a formal complaint, email us info@walletto.eu. We will provide an answer within 15 (fifteen) working days of receiving your question, unless in exceptional cases where it is not possible to provide an answer within 15 working days, we may take up to 35 (thirty five) working days to respond and notify you separately.

19.5. If you are a Consumer and you considers that your complaint has been resolved incorrectly, you have the right to complain directly to the institution supervising us - the Bank of Lithuania. A complaint to the Bank of Lithuania can be submitted in the following ways:
19.5.1. via the electronic dispute resolution tool E-Government Gateway; 19.5.2. by filling in the User's application form, which can be found on the Bank of Lithuania's website and sending it to the Law and Licensing Department of the Bank of Lithuania, Totorių st. 4, 01121 Vilnius, e-mail prieziura@lb.lt;
19.5.3. by filling in a free-form application and sending it to the Law and Licensing Department of the Bank of Lithuania, Totorių st. 4, 01121 Vilnius, e-mail prieziura@lb.lt;
19.5.4. More information about the procedure of submitting the compliant to the Bank of Lithuania may be found at
https://www.lb.lt/en/dbc-settle-a-dispute-with-a-financial-service-provider.

19.6. If you would like to contact us for any reason related to these Walletto General Terms and Conditions other than those described above, you may contact us by email info@walletto.eu.

19.7. In the event that the dispute cannot be resolved through negotiations, the disputes shall be settled in the courts of the Republic of Lithuania in accordance with the procedure established by the laws of the Republic of Lithuania.

20. Final provisions

20.1. You may not assign any of your rights under these Terms to a third party without our prior written consent.

20.2. You and we are independent contractors under these Walletto General Terms and Conditions and nothing here shall be construed as a partnership, joint venture or agency relationship between us.

20.3. If any court of competent jurisdiction finds any provision of these Walletto General Terms and Conditions to be invalid, illegal or unenforceable, that provision will be severed from the remainder of these Terms and Conditions, which will continue in full force and effect to the extent permitted by law.

20.4. The Parties shall immediately inform each other of all circumstances relevant to the proper implementation of these Walletto General Terms and Conditions. At our request, you must indicate the following circumstances (for example, in the event of a change in the signature of a legal representative, the opening and filing of bankruptcy proceedings, reorganization, reorganization, etc.), regardless of whether this information has been provided to public registers.

20.5. To protect your funds from possible illegal actions by third parties, you must immediately notify us in writing of the theft or other loss of your identity document.

20.6. The Parties shall promptly notify each other of any changes in their contact details. At our request, you must provide the relevant documents proving that the contact information has changed. Failure to comply with these obligations shall mean that the notice sent on the basis of the most recent contact information provided to the other Party has been duly served and that any obligation fulfilled on the basis of such contact information has been duly fulfilled. You acknowledge that we have the right to notify you of a change in our contact information by posting it publicly.