Approved by FSV Money Pte. Ltd.

Maxim Ignatichev, Director

QMC Privacy Policy

This Privacy Policy governs Client's use of products, services, content, features, technologies or functions offered by FSV Money Pte. Ltd., and all related sites, applications, and services (including, without limitation, when Client provides any information in relation to Client's use of QMC).

Client accept and consent to this Privacy Policy when Client signs up for, access, or uses the Money Pte. Ltd. By accepting and consenting to this Privacy Policy, Client expressly consents to our use and disclosure of Client's personal information and direct us to do so in the manner described in this Privacy Policy.

Client hereby declares that where Client has provided information regarding any other person (such as a Legal representative, an Authorized person, a Beneficial Owner or other similar data subjects), Client has provided such personal data to us only after Client has provided said data subject with the text of the present Privacy Policy and Client has obtained the consent for disclosure of the personal data of such other person to us.

1. General

1.1. This Privacy Policy is inseparable part of all Legal Agreements, that apply for Client's use of the QMC, including but not limited to the User Agreement for FSV Money Pte. Ltd, the Legal Agreement for QMC Account, provided by the respective Financial Institution, the Legal Agreement for QMC Card, provided by the respective Issuer and other legal documents (if applicable). We, meaning all parties, proving services to You (herein after also called "Client") under the above mentioned Legal Agreements. In the following Privacy Policy, we inform the Client about the collection, use and processing of Client personal data when applying, registering or using our FSV Money Pte. Ltd and all elements, included in the Service, including our website https://www.quickmoneyclick.com (hereinafter: "Website") and our QMC Mobile App, E-money account and Cards, jointly referred to as "Service".

All customer data is collected, transferred and maintained in accordance with the principles incorporated within applicable legislation as per the Legal Agreement and within the EC Directive 95/46 on the protection of personal data. The personal data regarding the Client that is provided by the Client as well as by third parties such as state and international authorities, which have competence in the prevention of frauds, is preserved in electronic form on servers, collocated in specially designed premises class A with the highest level of communication coverage, security and control of access.

1.2. Client has to read this Privacy Policy carefully in order to understand our views and practices regarding Client personal data, how it is used and how it is treated by us. Client has to download and save this Policy. If Client does not agree with this Privacy Policy, Client must not use our Service (as defined in the Legal agreements. By providing personal information to us and by maintaining contractual relations with us after Client has already obtained knowledge of this Privacy Policy, we will assume that Client has consented to the collection, use and disclosure of personal information about the Client in accordance with the terms set out in this Privacy Policy unless Client notifies us otherwise.

1.3. This Privacy Policy may be revised from time to time because new features may be added to our Service or because of amendments in legislation or other regulatory reasons. We may amend this Policy at any time by posting a revised version in the Mobile App or on the Website. The revised version will be deemed effective from the moment of its publication. In addition, if we propose to change this Privacy Policy in a substantial manner, we will provide the Client with at least 30 days prior notice of such a change via the Mobile App or via the Website for the Service. After the expiration of these 30 days, Client will be considered as having expressly consented to all amendments to the Privacy Policy. If Client disagrees with the terms of this Privacy Policy, Client may terminate its Agreement for the Service at any time according to the methods prescribed in the Agreement for the Service.

1.4. Not a Framework Contract: For the avoidance of doubt, this Privacy Policy does not constitute a "framework contract" for the purpose of the EU Payment Services Directive (2007/64/EC) or any implementation of that directive in the European Union or EEA (including, without limitation any national laws implementing the EU PSD).

2. Collection of Information

2.1. Collection and processing of Information in case of opening and using QMC Account

To open, maintain, use and close the E-money account and payment instruments, associated with the

Account and to use the Service provided by us, Client must provide:

● First name and surname ● Date of birth● Place of birth● Email address

● Nationality● Registered address● Mobile telephone number● Identification document● Type of identification document● Issue date● ID number● Issuing authority● or other details as may be requested.

Furthermore, for the purposes of funding the Account of the Client, Client may choose to provide information about its credit card, debit card or other payment instrument. We may generate and send to mobile phone number of the Client verification codes as well as to request the Client to enter them as a confirmation of certain actions. This required information is necessary for us in order to process transactions, issue new passwords (if applicable) in case the Client forgets or loses his/her password, in order to protect Client, us or other customers of ours against identity theft, credit card fraud as well as to contact Client should the need arise in administering the Account of Client. In order for us to provide our Service Client acknowledges and permits us his/her/its to have access to the contact list/address book, in the Client's smart phone in order to find, keep track and use of the mobile phone numbers of other users of the Services provided by us.

2.2. If Client sends to us correspondence, including post mails, e-mails and faxes, we will retain such information in the record made for the Account of Client. We will also retain customer service correspondence and other correspondence from us to Client. We retain these records in order to assess and improve the provision of customer service, as well as to investigate potential fraud and violations of the terms and conditions of the Service. In addition, phone calls from Client to us and vice versa will be monitored and/or recorded for purposes of quality improvement of the service, as well as for purposes of security and fraud detection.

2.3. In order to fulfill its legal obligations to prevent fraud and money laundering and/or to protect all of its customers against potential fraud, we may obtain information about Client from third party agencies, including financial history details, court judgments and bankruptcies, from credit reference and fraud prevention agencies when the Client opens Account and at any time when we deem necessary to protect from fraud or to minimize our financial risks. If the overall payment volumes which the Client sends or receives through the Service are high, in some circumstances we will conduct a background check on Client business by obtaining information about Client and its business from a Credit Reference or Fraud Agency. If Client owes us money, we may conduct a credit check on Client by obtaining additional information about the Client from a Credit Reference or Fraud Agency, to the extent permitted by law.

2.4. In addition to the personal information provided by the Client or obtained from third parties, our Service use a technology which allows us to gather particular technical information i.e. address of Client's internet protocol, operational system of the Client's computer, Client's browser type, traffic data, location data, weblogs and other communication data, whether this is required by us for purposes of control of risk and security, performance of regular obligations, inventory or other purposes. When Client accesses the Service using a mobile device (e.g. a smartphone), we may additionally collect and store device sign-on data (including device ID) and geolocation data in order to provide the services.

All personal information shall be recorded and kept on secured Microsoft cloud space and on our cloud on secured servers and shall be treated in compliance with the applicable AML/FT and

personal data protection laws.

3. Use of Information

3.1. By accepting this Privacy Policy, Client consents that we will use his/her/its personal information while providing its

services to Client including:

- To verify the identity and financial information of the Client;- To make fraud prevention checks, anti-money laundering/FT and credit checks;- For opening, operating and administering and closing the Account of the Client and the payment instruments associated to it and for provision of services that Client has requested;- For opening, operating and administering and closing of other Accounts, or services, or other payment instruments that Client has requested;- To execute instructions of the Client for undertaking and receiving payments and transfers using the Service, including for verifying that Client has sufficient funds in its Account and has any linked payment instruments to make such payment operations;- To notify the Client about changes to the service(s) provided by us;- To comply with financial and payment services regulations including retention of financial information and transactions information.- To exercise our rights and perform our obligations resulting from the Agreement with the Client;- To transfer our rights under the Agreement with the Client to a person established in a Member State of EEA, while at the same time complying with the provisions of the Agreement with the Client.

4. Disclosure of Information

4.1. We are not entitled to sell or rent any of personal information about the client to third parties in breach of its legal obligations. We will give access to the personal information about the Client only to those employees who need it in order to provide the Services to the Client. We may disclose personal information about the Client only in limited amount of cases explicitly listed in this document, as well as to the third parties and their sub-contractors, listed in the List of Third Parties with whom personal information may be shared, where the List is made available to the Client prior to entry into Agreement for the Service.

4.2. We may disclose personal information about the Client to third parties if it is necessary for us in order to, among other things, fulfill the request of the Client, process Client's payment details, provide support services and monitor fraudulent activities.

4.3. When Client sends money to another customer of the Service or a merchant to whom Client wishes to pay, we will, at a minimum, pass on to the recipient the mobile phone number, the e-mail address and the identification number of Account of Client. Depending on the type of payment involved, we may also send other personal details such as name, address and country of residence of Client if the recipients request this information from us in order to improve the payment process, to reconcile payments with the commercial transaction or to conduct their own anti-fraud and anti-money laundering checks.

4.4. We will also disclose information about Client to our auditing company which will carry out professional auditing services for us and will assess our policies for Anti Money Laundering (AML) and Know Your Customer (KYC).

4.5. We may disclose aggregated commercial data on turnovers made via the Service to third parties that act as our sub-contractors and have a contractual obligation to preserve the confidentiality and where this information will be used by them only for the purposes of distributing the Service and/or support of the Client for use of the Service.

4.6. We will disclose information about the Client in the event that we are obliged by an effective law to do so. Such disclosure includes, without limitation, transaction information, Account information, personal information and the contents of communications to: the court; the police; security forces; competent governmental, intergovernmental or supranational bodies; competent agencies (other than tax related authorities), departments, regulatory authorities. If false or inaccurate information is provided by Client and fraud is identified, we will pass details to fraud prevention agencies and law enforcement agencies may access and use that information. We and other organizations may also access and use this information (including information from other countries) to prevent fraud and money laundering.

Specifically:

a. Disclose necessary information to: the police and other law enforcement agencies; security forces; competent governmental, intergovernmental or supranational bodies; competent agencies, departments, regulatory authorities, self-regulatory authorities or organisations (including, without limitation, the Agencies referenced in the "Agencies" section of the Third Party Provider List here) and other third parties, including our Group companies, that we are legally compelled and permitted to comply with, including but without limitation the applicable laws on automatic exchange of information, such as Foreign Account Tax Compliance Act ("FATCA") or Common Reporting Standard ("CRS"); we have reason to believe it is appropriate for us to cooperate with in investigations of fraud or other illegal activity or potential illegal activity, or to conduct investigations of violations of our User Agreement (including without limitation, Client's funding source or credit or debit card provider).

If Client is covered by the FATCA or CRS Law, we are required to give the Client a notice of the information about the Client that we may transfer to various authorities.

b. Disclose information regarding Client's use intellectual property right owners if under the applicable national law of an EU member state they have a claim against us for an out-of-court information disclosure due to an infringement of their intellectual property rights for which our Services have been used;

c. Disclose necessary information in response to the requirements of the credit card associations or a civil, administrative or criminal legal process.

d. Disclose necessary information to the payment processors, auditors, customer services providers, credit reference and fraud agencies, financial products providers, commercial partners, marketing and public relations companies, operational services providers, group companies, agencies, marketplaces and other third parties.

e. Disclose necessary information to Client's agent or legal representative (if applicable, such as the holder of a power of attorney that the Client has granted, or a guardian appointed by the Client).

f. Disclose aggregated statistical data with our business partners or for public relations. For example,

we may disclose that a specific percentage of our active users. However, this aggregated information is not tied to personal information.

g. Share necessary information regarding Client's use of QMC Service with third parties (if applicable) for their use for the following purposes:

i. Fraud Prevention and Risk Management: to help prevent fraud or assess and manage risk.

ii. Customer Service: for customer service purposes, including to help service Client's Accounts or resolve disputes (e.g., billing or transactional).

iii. Shipping: in connection with shipping and related services for orders of cards.iv. Legal Compliance: to help them comply with anti-money laundering and counter-terrorist financing verification requirements.

v. Service Providers: to enable service providers under contract with us to support our business operations, such as fraud prevention, bill collection, marketing, customer service and technology services. Our contracts dictate that these service providers only use Client's information in connection with the services they perform for us and not for their own benefit.

5. Information Security and Protection

5.1. We take the responsibility to ensure that the information about Client is secure. To prevent unauthorized access or disclosure of information we maintain physical, electronic and procedural safeguards that comply with applicable regulations to guard non-public personal information. Once the Client is logged into his/her Account, all internet communication is secured using Secure Socket Layer (SSL) technology with High-grade security Encryption. We restrict access to personally identifiable information of the Client only to employees who need to know that information in order to provide products or services to Client.

5.2. The security of the Account and the payment instrument of Client also relies on protection by Clients of its identifying credentials of the Account, the payment instruments or other functionalities of the service, including transfers via SMS. Client shall not share its identifying credentials with anyone. We will never ask Client to send its identifying credentials in an e-mail, although we may ask Client to enter this and other personal information in the Account of Client for the Service via the Website or via the Mobile App uploaded on the Client's smart device or in other way as may be required by the Service. Any e-mail or other communication asking Client to provide personal information via email, or linking to a website with a URL that does not begin with https://www.LeuPay.ey/ should be treated by Client as unauthorized and suspicious and should be reported to us immediately.

If Client does share its identifying credentials with a third party for any reason, including because the third party has promised to provide additional services to Client, the third party will have access to the Account of Client and to its personal information, and Client will be responsible for the actions taken by the third party by using Client identifying credentials. If Client believes someone else has obtained access to its identifying credentials, must change it immediately by logging in to the account of the Client via the Website or via the Mobile App Profile of the Client and changing its settings, as well as to contact the our Customer

6. Contact with Client

6.1. We communicate with our Clients on a regular basis via email SMS or push notifications via the Website or via its mobile applications to provide its services. We also communicate with Clients by e-mail or phone to resolve customer complaints or claims made by Clients; respond to requests for customer service; inform Clients if according to us their Accounts or any of their transactions have been used for an illegitimate purpose; confirm information concerning a Client's identity, business or Account activity; conduct customer surveys; investigate suspicious transactions.

6.2. We use Client's email, physical address or mobile phone to send an SMS, email or push notification to confirm the opening of an E-money account, to send notice of payments that sent or received through us, to send information about important changes to the products and services, and to send notices and other disclosures required by law. We will monitor and/or record telephone conversations with Client to offer additional security, detect fraud and take instructions by Clients correctly or to resolve complaints.

7. Accessing and Changing Information by Client

7.1. Client can review the personal information which is provided to us and make any desired changes to such information, or to the settings for the Account of Client, at any time by logging in its account via the Website or the Mobile App and changing the.

7.2. If Client closes its Account, we will mark in its database the Account of Client as "Closed", but will keep the information about Client, as we are required to retain certain records for a period of at least five years after closure. This is necessary in order to detect fraud, by ensuring that persons who try to commit fraud will not be able to avoid detection simply by closing their Account and opening a new Account. However, if Client closes its Account, the personally identifiable information about Client will not be used by us for any further purposes, nor sold or shared with third parties, except as necessary to prevent fraud and assist law enforcement, or as required by law.

7.3. At the request of Client, we will also share with Client where the personal information of Client has been stored, what personal information we have about Client and for what purposes we use it. Client has legal right to such requests. They may be submitted to our Customer Service.