LIBRA GROUP

Anti-Corruption, Bribery and Money Laundering Policy and Procedures

October 2023

LIBRA GROUP

Contents

1 Introduction

1.1 Statement of Group Policy

Countries in which Libra Group (the 'Group') conducts business have adopted anti-corruption laws designed to combat the bribery, or other improper influence, of persons including, but not limited to, public officials. Anti-corruption laws typically include both anti-bribery prohibitions as well as financial record-keeping requirements. Anyone who breaks those laws can be subject to serious criminal and civil penalties including imprisonment, criminal fines, civil penalties, disgorgement of profits, and asset forfeiture.

The Group operates a zero-tolerance policy to bribery and corruption. It expects its employees and business partners to maintain the highest standards of ethical conduct and integrity and to comply with the letter and spirit of all applicable laws, regulations, treaties, and conventions.

1.2 Applicable laws

The Group designed this Anti-Corruption and Anti-Money Laundering Policy and Procedures document ('this Policy') to achieve compliance by the Group with anti-corruption and anti-money laundering laws of the countries with jurisdiction over:

(a) the Group's business; and

(b) its directors, officers, employees (staff, contract and temporary) ('Libra Staff'), and any other individual who, or entity which, performs services for or on behalf of the Group (including intra-group services such as HR and IT and third-party representatives acting on behalf of the Group) (referred to in this Policy as 'Service Providers' and, together with Libra Staff, 'Associated Persons').

The applicable anti-corruption laws include, among others:

(c) measures which have been adopted to implement national and international conventions and guidelines, including the United Nations Convention Against Corruption ('UN Convention'), the Criminal Law Convention Against Corruption of the Council of Europe (Criminal Law Convention), the Office of Economic Co-operation and Development Convention on Combating Bribery of Foreign Officials in International Business Transactions ('OECD Convention'):

(d) the Financial Action Task Force ('FATF') 40 Recommendations and 9 Special Recommendations establishing globally-accepted standards for anti-money laundering;

It is important to note that the Applicable Laws do not relate only to the bribery of public officials. Bribery of private citizens is illegal too. This Policy, therefore, applies to bribery of any person regardless of their capacity or status.

The Applicable Laws typically include anti-bribery prohibitions as well as financial record-keeping requirements. Violations of these requirements could result in significant criminal and civil liability for the Group and any of its Associated Persons who commit such violations.

1.3 Who this Policy applies to

Strict compliance with the requirements of the Applicable Laws and this Policy is mandatory for all Libra Staff and, if required by the terms of their engagement with the Group, Service Providers.

All Libra Staff and those Service Providers which are required to do so by the terms of their engagement with the Group must review and adhere to this Policy as a condition of their employment or engagement.

All Libra Staff and those Service Providers which are required to do so under the terms of their engagement with the Group must certify that they have read, understood, and agree to comply with this Policy.

Any Associated Person who knowingly fosters illegal conduct, ignores suspicious circumstances, or fails to comply with the Applicable Laws or this Policy and related procedures will, in the case of officers or employees of the Group, be subject to discipline, including possible termination for cause and may, in the case of Service Providers, be subject to contractual penalties including possible termination of their engagement.

1.4 Bribery prevention training

The Directors of Libra Group require ethical business practices and compliance with all Applicable Laws. In this regard, this Policy emphasises the Group's commitment to bribery prevention training.

General bribery prevention training is mandatory for all Libra Staff. It shall take the form of education and awareness raising about the threats posed by bribery in general and the various ways it is being addressed by the Group.

More advanced training may be provided to certain Libra Staff, tailored to the specific risks associated with specific roles. Refresher training shall be provided from time to time as required and at least every 12 months.

The Group shall also, where appropriate, provide advanced bribery prevention training and refresher training to Service Providers who represent a higher degree of risk from a corruption perspective. Where the Group does not train such Service Providers itself, it shall encourage the relevant Service Providers to conduct their own bribery prevention training.

2 Responsibility for Compliance

2.1 Chief Risk and Compliance Officer

Questions about this Policy should be directed to the Chief Risk and Compliance Officer.

The Chief Risk and Compliance Officer shall be responsible for overseeing the day-to-day implementation of this Policy, such as:

(a) Circulating, on a regular basis, to those Associated Persons deemed appropriate, a request for information regarding any gifts and hospitality which such persons may have given or received from business contacts during the previous quarter; and

(b) conducting risk assessments and the appropriate level of due diligence on third parties with whom the Group is proposing to enter into contracts.

The Chief Risk and Compliance Officer must request a determination from the Board in all cases where a high risk of bribery has been identified.

The Chief Risk and Compliance Officer shall:

(a) assist or decide (as appropriate) in respect of any matter referred to them;

(b) investigate possible violations or legal issues relating to this Policy;

(c) consult with legal counsel, as appropriate, to address inquiries regarding, or violations of, this Policy;

(d) inform the Group Chief Executive Officer, and, as appropriate, the Board of Directors of legal issues;

(e) make recommendations to the Chief Executive Officer and, as appropriate, the Board of Directors as to appropriate action to take to address possible violations or legal issues; and

(f) provide an annual compliance report to the Chief Executive Officer and, as appropriate, to the Board of Directors.

2.2 Notification of suspected violations

Any suspected violation of the Applicable Laws or this Policy should be immediately be brought to the attention of the Chief Risk and Compliance Officer.

The Chief Risk and Compliance Officer shall take any further action deemed necessary and appropriate, including considering whether to engage legal counsel to conduct a privileged and confidential internal investigation. No further action should be taken by the Associated Person until a response is received from the Chief Risk and Compliance Officer.

2.3 Whistleblower protection

This Policy prohibits retaliation in any form against individuals who, in good faith, report concerns about possible violations.

The Group shall not retaliate, nor shall the Group permit any member of Libra Staff to retaliate, against individuals who raise good faith reports of possible impropriety to management or the Chief Governance and Sustainability Officer or the Chief Risk and Compliance Officer.

The Group encourages individuals to put their name on any reports they make. It may otherwise be difficult to conduct an investigation that is meaningful and fair to all concerned.

More detail in connection with Whistleblower protection is provided in the Group's full Whistleblowing Policy.

2.4 Annual Compliance Review

The Chief Risk and Compliance Officer shall conduct an annual review in order to determine whether this Policy is fully understood and is being complied with and properly implemented (the 'Annual Compliance Review').

The Annual Compliance Review shall be presented to the Chief Executive Officer and, as appropriate, to the Board of Directors.

More frequent reviews may be warranted if an Annual Compliance Review reveals material issues of non-compliance or indications that this Policy has not been fully understood and/or implemented.

2.5 Record Retention

The Group shall maintain copies of all records and communications to document the implementation and operation of this Policy for as long as it considers appropriate and in compliance with applicable laws.

Records may take the form of memoranda, e-mails, audit reports, or other information that documents the operation of this Policy. Confidential records shall not be disclosed other than as permitted or required by law.

2.6 Cooperation with Law Enforcement

The Group is committed to cooperating with law enforcement and governmental authorities in accordance with Applicable Laws and regulations, and with due consideration for the privacy of clients and transaction counterparties.

The Group may be served with legal process (for example, a subpoena) or receive a written or oral request for information from law enforcement or other governmental authority in connection with investigations or inquiries that relate to potential corruption or money laundering.

Any member of Libra Staff served with legal process or who receives a written or oral request for information from a governmental agency or regulatory authority must refer the matter immediately to the Group General Counsel, the Chief Risk and Compliance Officer, or the Chief Executive Officer. Only those persons, or their delegates, are permitted to respond to legal process or other requests for information and to communicate with governmental authorities with respect to such inquiries.

3 Anti-corruption policies and procedures

3.1 Policy regarding travel benefits, gifts, and hospitality

Bona fide hospitality and promotional or other business expenditure that seeks to enhance the image of the Group, better present its operations, or establish cordial relations, is recognized as an established and important part of doing business.

It is not the intention of the Applicable Laws to criminalize such behavior. It is, however, clear that hospitality and promotional or other similar business expenditures can be employed as bribes.

This may be more likely if the travel benefit, gift, or hospitality in question is disproportionately generous.

No travel benefit, gift, or hospitality shall be given in exchange for a business benefit or any improper business advantage. Nor should it be given if it is intended to influence, or could be perceived as influencing, a business decision by the recipient.

Any gift must be in accordance with Applicable Laws and local laws, modest in value, promotional in nature, appropriate for the occasion, and customary or ceremonial in nature. Where practicable, it is recommended that gifts bear the Group logo.

Cash gifts to business contacts are expressly prohibited, as are cash equivalents, such as gift vouchers.

An Associated Person may receive from their business contacts or offer or give to a person who is not a public official, any gift or hospitality which does not exceed $50 in value for each gift or $250 in value per head for each hospitality event (not to exceed a total value of $2500 in any financial year). Any such gift-giving shall be properly recorded in the corporate books and any such gift-receiving shall be declared in writing to the Chief Risk and Compliance Officer upon request.

Associated Persons who wish to offer or give a gift or hospitality which does not fall within the above criteria must seek and obtain prior approval from the Chief Risk and Compliance Officer.

(a) date of the proposed hospitality/gift;

(b) names of each provider(s) and each recipient(s) of the hospitality/gift;

(c) the nature of the hospitality/gift (for example, 'wine tasting event at [x]');

(d) the purpose of the hospitality/gift (for example, 'developing a business relationship with [x]');

(e) the 'per head' spend on each non-Group recipient;

(f) confirmation that the offer or acceptance of the hospitality/gift is not intended to influence a decision-maker to award or obtain a business advantage improperly (for example that, as far as the person making the request is aware, there is no forthcoming pitch, tender, contract renewal or other formal decision process).

In no case shall Associated Persons pay for or reimburse the travel or lodging of the family or friends of the third party. The Group shall not fund or reimburse any 'side trips' for third parties.

3.2 Policy regarding benefits to public officials

The following issues arise in relation to the provision of travel benefits, per diems, gifts, and hospitality to public officials. They are to be considered in addition to the matters set out in Section 3.1.

Associated Persons must not offer or give any travel benefit, per diem, gift, or hospitality to any public official, except that:

(a) gifts may be given to such persons on or around a recognized gift-giving period, so long as the gift-giving is properly recorded in the Gifts and Hospitality Register and the nature and value of the gift accords with

local norms. For example, the giving of sheep and sugar during Ramadan is acceptable; or

(b) a travel benefit, per diem, gift, or hospitality may be given to such persons with the express prior written approval of the Chief Risk and Compliance Officer. The Chief Risk and Compliance Officer will consider matters including:

(i) the nature and value of the travel benefit, per diem, gift, or hospitality;

(ii) the circumstances of the occasion;

(iii) the legality of the provision of the travel benefit, per diem, gift, or hospitality under Applicable Laws and local law;

(iv) the frequency of travel benefits, per diems, gifts, or hospitality to any particular public official; and

(v) whether any travel which is at the invitation or request of the Group is for a bona fide business purpose or in the performance of a particular contract.

If the Chief Risk and Compliance Officer gives approval, the travel benefit, per diem, gift, or hospitality must be properly recorded in the Gifts and Hospitality Register.

3.3 Facilitation payments and kickbacks

Facilitation payments are a form of bribery made for the purpose of expediting or facilitating the performance of a public official for a routine governmental action, and not to obtain or retain business or any improper business advantage. Facilitation payments tend to be demanded by low-level officials to obtain a level of service to which one would normally be entitled to and must not be paid.

3.4 Use of Group assets and accuracy of financial records

Group assets may only be utilized in accordance with authorization by management.

All Libra Staff and those Service Providers which are required to do so under the terms of their engagement with the Group must maintain accurate accounting records and implement and maintain a system of internal controls to provide accountability for assets.

The Group requires that all financial transactions be accurately reflected in the Group's financial records and in accordance with generally accepted accounting principles.

The Group and all Libra Staff, together with those Service Providers which are subject to such a prohibition under the terms of their engagement with the Group, are prohibited from maintaining undisclosed or unrecorded funds or assets established for any purpose. Examples of undisclosed or unrecorded funds or assets include, but are not limited to, the following:

(a) numbered foreign bank accounts;

(b) bank accounts containing Group funds but held in the names of individuals;

(c) unrecorded petty cash or 'black box' funds; or

(d) real and personal property held by a nominee.

3.5 Prohibited means of payment

Associated Persons may not make a payment to an individual, representative, consultant, distributor, or other party unless an approved contract is in place. No payments shall be made in cash, to numbered accounts, to third-country accounts, or third-party accounts unless specifically authorized by the Group Financial Controller, who shall liaise with the Chief Risk and Compliance Officer as appropriate. All payments must be supported by properly documented invoices.

Checks may only be written to 'cash' or 'bearer' where the Group has received an invoice in respect of the relevant payment and a receipt from the payee. Such payment, together with copies of the relevant invoice and receipt, must be properly recorded in the corporate books.

3.6 Charitable donations and political contributions

Associated Persons are only permitted to utilize Group assets or resources for charitable donations or political contributions subject to the express authorization of the Chief Risk and Compliance Officer who shall base any such approval on the law of the jurisdiction where the donation is to be made, considering the amount, timing, and means of the contribution. The Chief Risk and Compliance Officer shall maintain records of any such approvals in the Group files.

3.7 Doing Business through Investments or Transactions with Business Partners

The Group requires that all investments and transactions involving its Business Partners be memorialized in writing. Any proposed business transaction involving public officials or state-owned businesses shall be subject to heightened due diligence. This may include commissioning an investigation agency to provide a report on any intermediaries who shall be liaising with public officials on behalf of the Group.

3.8 Further guidance

Inquiries concerning this Policy should be directed to the Chief Risk and Compliance Officer.

4 Anti-corruption procedures regarding third parties

4.1 Background

From time to time, the Group may deem it necessary, reasonable, or prudent to engage third parties to provide services to it.

Before the Group enters into contractual relations of any kind with any third party it shall, first, assess the risk of that person committing acts of bribery on its behalf and, secondly, conduct an appropriate level of due diligence on that person.

Third parties may only be engaged after the completion of the processes and any relevant approvals have been granted as detailed in this Section 4.

4.2 Initial business justification and third-party identification (STEP I)

The Group must assess and document the legitimate business need and justification for engaging a new third party.

Prior to engaging a new third party, the relevant business unit shall categorize the third-party by the size of the contract as follows:

(a) **Tier 1 Counterparties**: those where the total value of the proposed contract/engagement is reasonably anticipated to be less than US$5,000 in any twelve (12) month period; and

(b) **Tier 2 Counterparties**: those where the total value of the proposed contract/engagement is reasonably anticipated to be in excess of US$5,000 in any twelve (12) month period.

The relevant business unit shall not be obliged to categorize any third party as described in Section 0 if the Chief Risk and Compliance Officer has decided that there is a low risk of the relevant third party committing acts of bribery on the Group's behalf after having conducted an appropriate level of due diligence. For example, the appropriate level of due diligence to be conducted by the Group shall be low when contracting for IT, catering, or cleaning services involving an internet search for adverse reports to reflect the low risk of such service providers committing acts of bribery on the Group's behalf.

For any Tier 1 Counterparties, where both of the following statements are confirmed as correct:

(c) the third party is not dealing with public officials on behalf of the Group; and

(d) the third party is a corporate entity that is not a personal service Group (that is, a Group that provides the services of an individual and is owned and operated by that individual, such as a contractor selling their services through a limited Group),

then there is no requirement to conduct anti-corruption due diligence. However, if there are any concerns in relation to an arrangement that falls within this exemption from the requirement to conduct anti-corruption due diligence from a money laundering perspective, then they should be raised with the Chief Risk and Compliance Officer as soon as possible.

For any Tier 1 Counterparties where one or both of the statements set out in Sections (c) and (d) is not correct then such Tier 1 Counterparties shall be treated as a Tier 2 Counterparty for the purposes of this Section 4.

For all Tier 2 Counterparties, the relevant business unit shall prepare a brief internal memorandum ('**Initial Assessment**') which shall be used to justify the business rationale for engaging with the third party.

The Initial Assessment shall describe all material, relevant information and include:

(e) scope and timeline of the work to be undertaken;

(f) legal name of the third party (and if a subsidiary, name of the main parent Group and ownership percent) and key contact (if different);

(g) anticipated total size of the contract to be awarded in local currency (and in US dollars equivalent), if any element of the compensation is linked to securing business for the Group, and length of the engagement;

(h) how the third party became known to the Group;

(i) rationale behind the selection of the third party and summary of any selection process undertaken;

(j) relevant experience of the third party and expected benefits of the engagement with the third party;

(k) reporting lines and monitoring process for the third party by the Group;

(l) whether the third party shall be given any authority to act on the Group's behalf; and

(m) whether the third party shall be engaged to assist with any processes required by public officials (e.g. securing of visas, getting materials through customs, etc.).

The Initial Assessment shall not be deemed to be approved until it has been signed off by the Chief Risk and Compliance Officer. The Chief Risk and Compliance Officer shall not sign off the Initial Assessment unless it is satisfied that there is appropriate justification for engaging the third party.

Following approval of the Initial Assessment, the relevant business unit will carry out the due diligence and internal risk rating process as summarised in Section 4.3 below.

The Group shall not be required to repeat the procedure set out in this Section 4 in relation to a third party if that party is an existing third-party service provider applying for a substantially similar role in the future, unless:

(n) the third party was originally assessed more than two years previously;

(o) the third party was originally assessed as presenting a high risk from a bribery perspective; or

(p) the Group is otherwise aware that the third party now presents an increased risk from a bribery perspective.

However, if there are any concerns in relation to an arrangement that falls within this exemption from the requirement to conduct anti-corruption due diligence from a money laundering perspective, then they should be raised with the Chief Risk and Compliance Officer as soon as possible.

4.3 Due diligence and internal risk rating process (STEP II)

Before entering into a contractual relationship with a Tier 2 Counterparty, the Group shall follow the anti-corruption process set out in its Risk Assessment Procedures Document (as amended from time to time). This process is summarised in this Section 4.3.

Requests made as part of the due diligence process should involve direct communications with the third party, internet-based research, and, where appropriate, the use of a third-party due diligence provider.

Any concerns regarding findings from the due diligence process (or otherwise) relating to a third-party service provider shall be reported directly to the Chief Risk and Compliance Officer.

Please refer to Schedule 5 for example indicators of potential bribery risks.

Tier 2 Counterparties

For third parties categorized as Tier 2 Counterparties, the following information shall be ascertained:

(a) legal name and contact details of the third party;

(b) if the third party is an individual, his/her date of birth and employment status;

(c) if the third party is a corporate entity, its registered address, details of its ownership structure, and details of any party with an ownership interest of more than 25%;

(d) bank account details (including full name and location of bank);

(e) details relating to the proposed method for payments;

(f) if a public official or any family relation of a public official has an ownership interest in the third party;

(g) if a public official or any family relation of a public official recommended the third party to the Group;

(h) if there are any sanctions or trade restrictions against the third party;

(i) if the third party intends to utilize a particular employee or third party to carry out work on its behalf, and if so the relevant details;

(j) a review of the third party's Group brochures or website materials (if available);

(k) a Google search for international and local press accounts to see if the third party has been in the press associated with an ethical or corruption scandal; and

(l) a World Check search on the third party, being an individual, or key stakeholders if it is a corporate entity,

In respect of Tier 2 Counterparties whose shares are publicly traded on one or more of the following stock exchanges: (i) New York Stock Exchange, (ii) NASDAQ OMX, (iii) London Stock Exchange, (iv) Tokyo Stock Exchange, or (v) Shanghai Stock Exchange, only the information set out in Section 0 (a), (c), (g), (h), (i), (j), (k) and (l) needs to be ascertained.

Internal risk rating

An initial internal risk rating of 'Low', 'Medium' or 'High' shall be assigned to each third party based on the answers to the due diligence questions. If a third party is required to undergo 'Enhanced Diligence' in accordance with Section 4.4 a final internal risk

rating of 'Low', 'Medium', or 'High' shall be assigned to the third party based on the outcome of the Enhanced Diligence process.

Any third party assigned an initial internal risk rating of 'Low' shall be presented to the Chief Risk and Compliance Officer for approval to enter into a contractual arrangement with the third-party service provider.

Any third party assigned an initial internal risk rating of 'Medium' or 'High' shall be subject to a further level of Enhanced Diligence as set out below.

4.4 Enhanced diligence (STEP III)

Any third party which is assigned an initial internal risk rating of 'Medium' or 'High' shall be subject to a further set of Enhanced Diligence questions so that the Group can fully assess the suitability of the third party for the proposed work and identify any specific areas of risk.

The Enhanced Diligence questions shall be informed by the findings of the initial due diligence exercise carried out in accordance with Section 4.3 and as such, the questions will be tailored according to the areas of risks identified which may include, but shall not be limited to, requesting:

(a) the full names and dates of birth of persons who have ownership interests in the third party of 25% or above and if considered appropriate, citizenship information and CVs;

(b) details of how the third party is organized and confirmation that the third party has been validly incorporated and registered under local laws;

(c) details of any parent companies or trusts;

(d) details of the third party's business activities, key clients/contracts, and geographical areas of operations;

(e) if the third party has any past criminal convictions (especially in the areas of tax evasion or bribery); any bankruptcies; and any cases of civil litigation in which the third party has been a defendant;

(f) audited financial statements or tax returns if available, or at least a financial reference in cases where there is any doubt as to the third party's ability and resources to provide the services in question; and

(g) the following information, with supporting documentation,

  (i) a reasonable number of business references (if applicable) so that the Group may have an independent account as to the third party's effectiveness, standing in the community, and reputation for ethical business practices; and

  (ii) if financial statements or tax returns are unavailable or do not provide a complete picture, financial references from the third party's bank(s).

Following the Enhanced Diligence if the third party is assigned a final internal risk rating of 'Low' or 'Medium' it shall be presented to the Chief Risk and Compliance

Officer for approval to enter into a contractual arrangement with the third-party service provider.

In general, barring an omission or manifest error during the initial internal risk assessment, a third party that is assigned an initial internal risk rating of 'High' would be highly unlikely to be assigned a final internal risk rating of 'Low' following Enhanced Diligence.

The Group will only transact with a third party which is assigned a final internal risk rating of 'High' if approved by the Board which, having reviewed the third party contract in conjunction with the Risk Assessment Procedures Document (as amended from time to time) have concluded that the risk of the third party committing acts of bribery on behalf of Libra is limited and this risk has been appropriately mitigated through contractual warranties or otherwise

Any third party not approved under Section 4.3 or Section 4.4 shall be barred from reapplying for the same or a substantially similar role for a minimum period of 6 months (unless the Chief Risk and Compliance Officer determines otherwise) and shall, regardless of the role which the third party applies for, be subject to Enhanced Diligence.

If a member of Libra Staff believes that a third party is engaging in corrupt activity, he or she must immediately notify the Chief Risk and Compliance Officer or the Chief Executive Officer. It is the responsibility of the Chief Risk and Compliance Officer to examine the activity and to determine the appropriate course of action, including, in consultation with legal counsel, the reporting of corrupt activity to government authorities in accordance with Applicable Laws and regulations.

4.5 Contract terms

All third parties must be engaged by the Group through a formal written contract. The contract must, at a minimum, address the following elements:

(a) compensation structure;

(b) any discounts;

(c) the types of services being performed;

(d) whether fees are tied to results (such as the Group entering into a contract) in the form of commissions or paid on a flat-fee basis;

(e) anti-corruption provisions appropriate to the bribery risk which the third party presents to the Group; and

(f) the provision by the third party of anti-corruption certificates at the Group's request.

4.6 Monitoring

The Group shall monitor the third party's activities after engagement.

The Chief Risk and Compliance Officer shall conduct an annual review in order to ascertain whether the Group's assessment of the bribery risk which each third party presents to the Group remains valid.

Reviews and audits may also be conducted as necessary at the discretion of the Group. When conducting such reviews and audits the Group may consider any matters which it deems appropriate, including but not limited to the issues highlighted in this Section.

4.7 Acquisitions of businesses or teams

When considering the acquisition of businesses, particularly those involving the acquisition of new employees, the Group shall undertake a due diligence process approved by the Chief Risk and Compliance Officer.

4.8 Risk assessment and anti-corruption due diligence

The main reasons behind the requirement for due diligence are as follows:

(a) to try to establish that third parties that in any way act on the Group's behalf are suitable for this purpose. The intention is to minimize any risk that a third party shall take any actions that could breach any anti-corruption laws for which ultimately the Group and Libra Staff could be held responsible;

(b) to try to ensure that the individuals and entities that the Group does business with are engaged in legitimate businesses. The purpose here is to minimize any risk that the Group engages with any person or entity engaged in money laundering or other illicit activities (see Section 6.1 regarding anti-money laundering due diligence); and

(c) to try to ensure that the Group does not have dealings with a third party that would result in the Group or Libra Staff coming 'into disrepute'.

4.9 Local legal framework

The laws of the jurisdiction in which the third party shall operate could affect how the Group may engage, utilize and terminate its contractual arrangements with the third party. The Group shall take appropriate legal advice in such circumstances.

5 Anti-money laundering policy

5.1 Background

The Group's goal is to conduct its operations in a manner that allows Libra Staff, facilities, products, and services to be used only for legitimate business purposes. The Group has adopted this Policy to educate Libra Staff about money laundering and to establish guiding principles and consistent global standards designed to protect the Group from being used to facilitate money laundering or other illicit activities.

Effective prevention begins with Libra Staff. Therefore, all Libra Staff must familiarize themselves with this Policy and understand how to prevent, detect, and refer suspicious activities and transactions to the Chief Risk and Compliance Officer for review and assessment.

5.2 What is Money Laundering?

Money laundering is broadly defined as the attempt to conceal the origin and ownership of the proceeds of illegal activity and to disguise assets to make them appear legitimate. Broadly, there are considered to be three stages to money laundering,

which may comprise numerous transactions by the launderers that could alert an institution to a criminal activity:

(a) ***placement*** – the stage where cash first enters the financial system and is converted into monetary instruments, such as money orders or travellers' checks, or deposited into accounts at financial institutions;

(b) ***layering*** – the stage where funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin; and

(c) ***integration*** – the stage where funds are reintroduced into the economy in such a way that the source of the funds appears legitimate.

Money laundering can involve the proceeds of any serious crime including, but not limited to, drug trafficking, insider trading, bribery, tax evasion, embezzlement, and securities, bank, wire, or mail fraud.

Money laundering transactions need not involve cash and can involve any type of financial transaction, including check deposits, withdrawals, transfers, or movements of funds, securities, or other property. Moreover, money laundering can consist of either a single transaction or a pattern of transactions, or complex activities.

In most countries, it is a crime to conduct or to assist in a financial transaction with 'knowledge' or 'wilful blindness' that the transaction involves the proceeds of criminal activity. 'Wilful blindness,' or the deliberate failure to ask questions when the suspicions of a member of Libra Staff are aroused, may result in the person being charged with the crime of money laundering to the same degree as if the person had been told explicitly that the funds were derived from criminal activity.

It is also illegal to receive funds with 'knowledge' that they are criminally derived.

It is a crime for a person:

(d) to conceal, disguise, convert, transfer criminal property, or remove criminal property;

(e) to enter into or become concerned in an arrangement that he/she knows or suspects facilitates (by whatever means) the acquisition, retention, use, or control of criminal property by or on behalf of another person;

(f) to acquire, use or possess criminal property; and/ or

(g) who knows or suspects that a money laundering investigation is being conducted or is about to be conducted to make a disclosure which is likely to prejudice the investigation or falsify, conceal, or destroy documents relevant to the investigation, or cause that to happen.

For the purposes of this Section 0 property is criminal property if the alleged offender knows or suspects that the property constitutes or represents benefit from a criminal conduct.

6 Anti-money laundering procedures

6.1 Anti-money laundering due diligence

The Group's goal is to only do business with counterparties engaged in legitimate business activities and who derive their income, wealth, funds, and investable assets from legitimate sources. By dealing only with such counterparties who are known to the Group through the implementation of proper due diligence efforts, the Group can minimize the risk of transacting business with or entering into joint ventures with, or on behalf of, a person engaged in money laundering or other illicit activities.

Consistent with this important objective, before establishing a business relationship with a counterparty or entering into any other business relationship on behalf of the Group, the Group, and Libra Staff must have:

(a) complied with all applicable Group procedures for establishing counterparty business relationships; and

(b) performed sufficient due diligence to be confident in the legitimacy of the proposed transaction, including the lawfulness of the transaction and the source of funds.

The Group has tailored its counterparty due diligence procedures to address the potential money laundering risks that may be associated with particular types of counterparties, jurisdictions, business lines, or methods of doing business.

The anti-money laundering due diligence process which must be followed by the Group prior to entering into a contractual relationship with a third party is summarised below.

There is no requirement to conduct anti-money laundering due diligence where:

(c) the total contract value is less than $5000; *or*

(d) the counterparty is not dealing with public officials on behalf of the Group.

However, if there are any concerns about an arrangement that falls within this exemption from the requirement to conduct anti-corruption due diligence from a money laundering perspective, then they should be raised with the Chief Risk and Compliance Officer as soon as possible.

Counterparties that have been categorized by the Group as presenting higher degrees of risk from a corruption perspective shall be required to provide more information and documentation in the context of the Group's anti-money laundering due diligence than those which have been categorized as presenting lower degrees of risk.

Before establishing a business relationship with a counterparty, effecting a transaction, or entering into a business transaction on behalf of the Group with a counterparty deemed to be at high risk, the Group requires higher levels of due diligence be performed and Libra Staff must check with the Chief Risk and Compliance Officer regarding any additional due diligence procedures that may be required.

The following factors may indicate that a third party should be considered as presenting a high risk from a money laundering perspective:

(e) individuals that are either current or former senior foreign or domestic political figures or are friends or relatives of current or former senior foreign or domestic political figures;

(f) individuals or entities that are domiciled in a jurisdiction that does not have effective anti-money laundering regimes or where there is a high incidence of corruption; or

(g) individuals or entities that have been included on a governmental or international organization's list of terrorists.

6.2 Detecting and referring suspicious activity

Libra Staff must be alert for possible money laundering or suspicious activity. Any member of Libra Staff participation in money laundering, either with knowledge or through wilful blindness, is strictly prohibited. Libra Staff must not advise or assist anyone who is attempting to avoid money laundering laws or circumvent this Policy and its implementing procedures.

Under no circumstances may any member of Libra Staff inform or 'tip off' any party involved in suspicious or illegal activity that his, her or its activities are believed to be suspicious, are being referred within the Group or reported to government authorities, or are being investigated by the authorities.

If a member of Libra Staff believes that a transaction is suspicious, he or she must immediately notify the Chief Risk and Compliance Officer or the Chief Executive Officer. It is the responsibility of the Chief Risk and Compliance Officer to examine the activity and to determine whether the activity is suspicious, with the goal that appropriate action is taken, including, in consultation with legal counsel, the reporting of suspicious activity to government authorities in accordance with Applicable Laws and regulations.

In the event that the person concerned by a potentially suspicious transaction is unable, or unwilling to notify the Chief Risk and Compliance Officer or the Chief Executive Officer then they should report the issue through one of the Whistleblowing channels provided.

6.3 Cash and cash equivalents

In order to reduce the risk of the Group's inadvertent involvement in money laundering schemes, the Group requires documentation of the handling of cash and cash equivalents (for example, checks, money orders, etc.). This documentation is designed to prevent money launderers from using the Group to evade cash and cash equivalent reporting requirements.

The Chief Risk and Compliance Officer shall review this documentation for suspicious activity that may implicate cash reporting requirements.