REMITTANCE RULES

Last updated: 11 January 2024

These rules (the "**Remittance Rules**"), in addition to the Terms and Conditions found in https://pdax.ph/terms-and-conditions, and all rules and policies incorporated therein by reference, shall govern your relationship with PDAX when creating, accessing, and using your PDAX Account for Remittance Activities, as defined below.

These Remittance Rules are deemed incorporated into the Terms and Conditions. In case of conflict between the Terms and Conditions and these Remittance Rules on matters relating to remittance activities, these Remittance Rules shall govern.

1. DEFINITION OF TERMS

The capitalized terms used herein which are defined in the Terms and Conditions, shall have the respective meanings assigned to them in the Terms and Conditions except as otherwise provided herein or unless the context otherwise requires. In addition to the definitions in the Terms and Conditions, the following definitions apply:

a. **GUI** refers to the Graphical User Interface.
b. **Remittance Activities** refer to activities relating to the transfer of funds, or the movement of funds or monetary instruments from the sender or originator to a receiver or beneficiary locally and/or internationally.
c. **User's Clients** refer to specific senders and corresponding receivers for whose benefit, the User avails of Services under the Terms and Conditions and these Remittance Rules.

2. GENERAL POLICY

The User is permitted to use the PDAX Account in order to conduct international Remittance Activities for User's Clients. You may only use these Services if you are specifically permitted to do so by PDAX. PDAX may promulgate operational guidelines to govern Remittance Activities and related activities, which shall be deemed incorporated into, and shall form part of, these Remittance Rules.

3. CERTIFICATION

For some Users covered by these Remittance Rules, Digital Assets or Fiat Currency transferred to, or withdrawn from, the PDAX Account, constitute an aggregated sum composed of various sums pertaining to the User's Clients. In these cases, the User hereby undertakes to execute a sworn certification in compliance with Applicable Laws and Rules, certifying that:

a. the User has conducted, is conducting, and will continue to conduct, the prescribed identification procedures for the User's Clients in accordance with the Applicable Laws and Rules, and the User's own Money Laundering/Terrorist Financing Prevention Program (MLPP), including face-to-face contact, personal interviews, and/or such Information and Communications Technology ("ICT") methods permitting customer identification in a similar manner, to validate the existence and establish the ultimate identity of the User's Clients;

b. if the standards of the country where the User is operating has User's Clients' identification process requirements which are less stringent than those of the Republic of the Philippines, the User shall follow the standards of the Republic of the Philippines, specifically with respect to customer due diligence, record keeping obligations, and the requirements prescribed in: (i) the AMLA and its implementing rules and regulations; (ii) Part Nine of Q-Regulations (Anti-Money Laundering Regulations) of the Manual of Regulations for Non-Banks Financial Institutions (MORNBFI), as may be amended from time to time; (iii) and related issuances of the BSP including but not limited to BSP Circular No. 706, as amended by BSP Circulars No. 950 and No. 1022 and as may be further amended from time to time (collectively, "Philippine AML/CTF laws");

c. upon request, the User shall inform PDAX of: (i) the jurisdictions where it has material operations; (ii) the nature of its business and reputation; (iii) the entities responsible for, and the quality of, its supervision, regulation, and monitoring; and (iv) any money-laundering or terrorist financing investigation or regulatory action which it may have been involved in;

d. the User has measures in place to conduct due diligence and record-keeping requirements in relation to the User's Clients in accordance with all requirements of all regulations enforced by the regulatory bodies of all jurisdictions where it operates;

e. the User has conducted, and continues to conduct the required screening of its users against established sanctions lists, *i.e.* the "Specially Designated Nationals and Blocked Persons" list maintained by the Sanctions Authorities, or any similar list maintained by, or public announcement of Sanctions designation made by them, including, the "Specially Designated Nationals and Blocked Persons" list maintained by the OFAC, the Consolidated List maintained by the UNSC, the Consolidated List of Financial Sanctions Targets and the Investment Ban

List maintained by HMT, those designated by the ATC, or any similar list maintained by, or public announcement of Sanctions designation made by any of the Sanctions Authorities;

f. the User has not, does not, and will not endorse or allow access to PDAX's Services any of the User's Clients who is a positive match in any of the aforementioned sanctions lists;

g. the User has not, at any time, been reprimanded cited, or subjected to regulatory examination or other similar actions on account of unsatisfactory, insufficient, inadequate Anti-money Laundering/Counter-Terrorist Financing policies, procedures or practices;

h. upon request, the User undertakes to provide PDAX with the identification documents of all of the User's Clients, including senders and receivers without delay. The User warrants that it has secured the consent of the User's Clients to share such information; and

i. the User permits PDAX to conduct periodic KYC reliance and MLPP (or equivalent MLPP procedures) account reviews as PDAX deems fit, and undertakes to provide additional documentation as may be necessary to fully accomplish reviews without delay.

The User acknowledges that PDAX has full discretion to terminate its Services in case of fraud, misconduct, misrepresentation, or breach of the foregoing certifications; breach by the User or the User's Clients of Applicable Laws and Rules, including but not limited to the AMLA, or other related rules and regulations promulgated by the BSP; or to protect the legitimate interests of PDAX.

4. LETTERS OF INSTRUCTION

a. The User may send remittance instructions via GUI, a set of API provided by PDAX (hereinafter referred to as "PDAX API") or, if necessary, execute a letter, or any other written or digital document that will contain: (i) process flow for quotes for and acceptance of conversion rates; (ii) the Parties' respective authorized sender(s) and receiver(s); (iii) Authorized Communication Channels for Quotes and acceptance; and (iv) authorized accounts for the transfer and remittance of Fiat Currency and Digital Assets (hereinafter referred to as "Letters of Instruction").

b. The User hereby irrevocably authorizes PDAX to act in accordance with and upon the instructions and orders given in accordance with the Letters of Instruction, unless otherwise amended. Should there be any conflict between the Letters of Instruction and any oral or written agreement between the parties, the Letters of Instruction shall be controlling.

c. When Letters of Instruction are sent by letter or other written or digital document, the parties must signify their conformity with the Letters of Instruction before it becomes binding.
d. PDAX's forms and other documents, including but not limited to, account opening forms and whitelisting forms may supplement or take the place of Letters of Instruction.

5. INDEMNITY AND LIMITATIONS OF LIABILITY

In addition to Section 17 (Limitation of Liability) and Section 18 (Indemnity) of the PDAX Terms and Conditions, applicable Platform Rules and unless as otherwise provided in a separate written agreement, User agrees to fully defend, hold harmless, and indemnify PDAX or the PDAX Group from and against all claims, disputes, settlements, awards, damages, losses, expenses and costs (including legal costs) suffered or incurred by PDAX or the PDAX Group, in connection with or arising from:

a. any dispute between or among the User, the User's Clients, and any entity to which the User may be related to or associated with through the use of the Services covered by these Remittance Rules;
b. any claim, demand, or suit that may be instituted by the User's Clients, or by any entity to which the User may be related to or associated with through the use of the Services covered by these Remittance Rules, against PDAX; and
c. any claim, demand, or suit between the User and its credit providers.

6. FEES

You may be charged additional fees for availing of this Service Fees which shall be communicated to you in writing before you are charged.

7. PERSONAL DATA PROTECTION

The User shall abide by all Applicable Laws and Rules in relation to personal data processing and the Privacy Policy.

To the extent that PDAX could potentially process the Personal Data of the User's Clients to facilitate Remittance Activities as defined herein, the User may be required to execute a notarized Data Outsourcing Agreement with PDAX to ensure compliance with Applicable Laws and Rules, in substantially the following form:

a. **Term** – The Data Outsourcing Agreement shall have the duration indicated in the DOD, as defined below.

b. **Adherence to the Data Privacy Act of 2012** –The Parties hereby adhere to the DPA, recognizing the importance of appropriate privacy protections for data subjects.

c. **Definitions**

(i) **DOD** refers to the Data Outsourcing Details, to be executed separately by the Parties, which contains the subject matter of processing, duration of processing, purposes of processing, Data Subjects and Personal Data types, geographic location of processing, and details of sub-contracting to third-parties.

(ii) **Personal Information** refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

(iii) **Sensitive Personal Information** refers to personal information:

- About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- Specifically established by an executive order or an act of Congress to be kept classified.

(iv) **Personal Data** refers to both personal information, sensitive personal information, and privileged information.

(v) **Processing** refers to any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system.

(vi) **Data Outsourcing** refers to the disclosure or transfer of Personal Data by a Personal Information Controller to a Personal Information Processor.

(vii) **DPA** refers to the Republic Act 10173, also known as, Data Privacy Act of 2012, its Implementing Rules and Regulations, and the issuances of the National Privacy Commission.

(viii) **Data Protection Officer** refers to any individual designated by the Personal Information Controller or Personal Information Processor who is accountable for compliance with the DPA.

(ix) **Data Subject** refers to an individual whose personal, sensitive personal, or privileged information is processed.

(x) **Security Incident** refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result in a Personal Data breach, if not for safeguards that have been put in place.

(xi) **Personal Data Breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. A Personal Data breach may be in the nature of:

- An availability breach resulting from loss, accidental or unlawful destruction of Personal Data;
- Integrity breach resulting from alteration of Personal Data; and/or
- A confidentiality breach resulting from the unauthorized disclosure of or access to Personal Data.

(xii) **Personal Information Controller** refers to a natural or juridical person, or any other body who controls the processing of Personal Data, or instructs another to process Personal Data on its behalf. The term excludes:

- A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
- A natural person who processes Personal Data in connection with his or her personal, family, or household affairs.

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.

(xiii) **Personal Information Processor** refers to any natural or juridical person or any other body to whom a personal information

controller may outsource or instruct the processing of Personal Data pertaining to a Data Subject.

(xiv) **Receiving Party** refers to the party to whom the Personal Data was disclosed to.

(xv) **Sharing Party** refers to the party disclosing the Personal Data.

(xvi) **Technical, Physical, and Organizational Security Measures, or TPOSM** refer to those measures aimed at protecting Personal Information transmitted, stored, or otherwise processed against improper, unauthorized, accidental or unlawful processing, destruction or loss, disposal, alteration, disclosure, or access, and against all other unauthorized and unlawful forms of processing.

d. **Roles of the Parties** – User is the Personal Information Controller of the Personal Data disclosed to PDAX. PDAX is a Personal Information Processor, *i.e.*, it processes such Personal Data upon the instruction of the User.

In the event that either party takes on the role of a Personal Information Controller or Personal Information Processor, as defined under the DPA, such party herein undertakes to implement the necessary measures, and execute its role as Personal Information Controller or Personal Information Processor, as the case may be, in relation to any Personal Data which comes into its possession by virtue of the Terms and Conditions and these Remittance Rules, in accordance with the DPA.

e. **Personal Data to be Collected and Processed** – PDAX shall process only the Personal Data listed in the DOD, in accordance with the terms of the Data Outsourcing Agreement.

The terms of the Data Outsourcing Agreement shall apply to Personal Data in all its forms. It may be on paper, stored electronically, held on film, microfiche, or other media. It includes text, pictures, audio, and video. It covers information transmitted by post, by electronic means, and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the data from creation, collection, storage, utilization, to disposal. The terms of the Data Outsourcing Agreement apply to all officers, employees, and clients of both Parties where they are performing their duties in relation to the Data Outsourcing Agreement.

f. **Purposes of Processing** – PDAX shall process the Personal Data only for the purposes listed in the DOD.

The User may, at any time and upon written instructions to PDAX, require PDAX to process the Personal Data pursuant to and consistent with the following purposes:

(i) Comply with statutory and regulatory requirements, including directives, issuances by, or obligations of User to any competent authority, regulator, supervisory body, enforcement agency, exchange, court, quasi-judicial body, or tribunal;
(ii) Enable User to exercise sound corporate governance over its businesses, ensure that risks arising therefrom are duly identified, measured, managed and mitigated, and enhance risk assessment and prevent fraud;
(iii) Enable User to conduct User audits or investigate a complaint or security threat;
(iv) Other legitimate business purposes of the User and PDAX;
(v) Establish, exercise, or defend PDAX's legal claims; or
(vi) Fulfill any other purposes directly related to the above-stated purposes.

g. Geographic Location of the Processing – The Personal Data shall be processed by PDAX at the geographic location specified in DOD.

PDAX shall, at least thirty (30) days prior to effecting any change in the geographic location, notify the User in writing of such intended change and provide reasonable proof that such change shall not adversely affect the TPOSM currently in place or impact the privacy rights of the Data Subjects.

h. Obligations of User – Pursuant to the requirements of the DPA, the User hereby undertakes to:

(i) Secure the written consent of each Data Subject;
(ii) Process Personal Data to the extent allowed by the Data Subject;
(iii) Specify the persons and/or entities authorized to receive, access, process, and/or transmit the information obtained and processed by PDAX, giving PDAX the right to refuse to give information to persons or entities not designated by User.

i. Obligations of PDAX – Pursuant to the requirements of the DPA, PDAX hereby undertakes to:

(i) Process Personal Data only upon the documented instructions of User, including transfers of Personal Data to another country or an international organization, to the extent contemplated under the

DOD, unless such transfer is authorized by Applicable Laws and Rules;

(ii) Ensure that an obligation of confidentiality is imposed on persons authorized to process the Personal Data;

(iii) Implement appropriate security measures and comply with the DPA;

(iv) Not engage another processor without prior instruction from User: provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;

(v) Assist the Personal Information Controller, by appropriate TPOSM and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;

(vi) Make available to the User all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections;

(vii) Immediately inform the User if, in its opinion, an instruction infringes the DPA;

(viii) Assist User in ensuring compliance with the DPA, taking into account the nature of processing and the information available to PDAX;

(ix) At the choice of the User, delete or return all Personal Data to the User upon termination of, and subject to, the Terms and Conditions and the Remittance Rules; and

(x) Report all available information to the User within forty-eight (48) hours from knowledge of, or reasonable belief that, a Personal Data Breach or a Security Incident has occurred, and extend full cooperation to the User to enable the User to comply with its obligations under the DPA.

j. **Security Obligations of PDAX** – Pursuant to its obligation to maintain the appropriate TPOSM, PDAX warrants that, at minimum, it shall have the following security measures:

Organizational Security Measures

(i) That it has a designated individual who functions as a Data Protection Officer.

(ii) That it has implemented appropriate data protection policies that provide for TPOSM, taking into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedoms of Data Subjects.

- The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.

- The policies shall implement appropriate security measures that, by default, ensure only Personal Data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of Personal Data collected, including the extent of processing involved, the period of their storage, and their accessibility.
- The policies shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.

(iii) That it shall maintain records that sufficiently describe its data processing system and identify the duties and responsibilities of those individuals who will have access to Personal Data. Records shall include:

- Information about the purpose of the processing of Personal Data, including any intended future processing or data sharing;
- A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the processing;
- General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of Personal Data;
- A general description of the TPOSM in place; and
- The name and contact details of each Party, its representatives, the sub-Users (if applicable), and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the Applicable Laws and Rules for the protection of data privacy and security.

(iv) That its employees shall operate and hold Personal Data under strict confidentiality. This obligation shall continue even upon termination of the employee's employment.

Physical Security Measures

(i) That it has implemented policies and procedures to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;

(ii) That the design of its office space and workstations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing Personal Data, taking into consideration the environment and accessibility to the public;

(iii) That the duties, responsibilities and schedule of individuals involved in the processing of Personal Data are clearly defined to ensure that

only the individuals actually performing official duties shall be in the room or work station, at any given time;

(iv) That it has implemented policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of Personal Data; and

(v) That it has implemented policies and procedures that prevent the mechanical destruction of files and equipment. The room and workstation used in the processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Technical Security Measures

(i) That it has implemented safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

(ii) That it has the ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

(iii) That it performs regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a Personal Data Breach;

(iv) That it has the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(v) That it has a process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

(vi) That it encrypts Personal Data during storage and while in transit, authentication process, and it has implemented other technical security measures that control and limit access.

k. **Indemnification** – User agrees to irrevocably, unconditionally, and fully indemnify and hold PDAX, the PDAX Group, its directors, officers, employees, sub-contractors, and agents, free and harmless from and against any and all claims, suits, actions or demands or losses, damages, costs and expenses including, without limiting the generality of the foregoing, attorney's fees and costs of suit that User may face, suffer or incur by reason or in respect of:

(i) User's or the User's Client's breach of any of the warranties and obligations set forth in the Data Outsourcing Agreement, regardless of the cause of such breach; or

(ii) Any act, omission or negligence of the User or the User's Clients that causes or results in the breach of obligations under the DPA.

l. **Data Subject Rights** – Each Party shall respect the following rights accorded to Data Subjects by the DPA:

(i) Right to be informed. Data Subjects have the right to be informed whether Personal Data pertaining to them shall be, are being, or have been processed, including the existence of automated decision-making and profiling. This Data Outsourcing Agreement may be accessed by the Data Subject upon written request submitted to any of the Parties.

(ii) Right to object. Subject to the limitations set forth in the DPA and other Applicable Laws and Rules, Data Subjects have the right to object to the processing of their Personal Data, including processing for direct marketing, automated processing or profiling. They may withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the Data Subject.

(iii) Right to access. Subject to the limitations set forth in the DPA and other Applicable Laws and Rules, Data Subjects have the right to request access to any of their Personal Data.

(iv) Right to rectification. Data Subjects have the right to dispute the inaccuracy or error in the Personal Data and have the PIC correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.

(v) Right to erasure or blocking. Subject to the limitations set forth in the DPA and other applicable laws and regulations, Data Subjects have the right to suspend, withdraw or order the blocking, removal or destruction of his or her Personal Data from the PIC's filing system.

(vi) Right to damages. Data Subjects have the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data, taking into account any violation of the rights and freedoms of the Data Subject.

(vii) Right to lodge a complaint with the National Privacy Commission.

m. **Communications Regarding Data Privacy Concerns** – For questions, requests, and notifications, communication may be directed to each

Party's designated Data Protection Officer or his/her replacement or substitute.

8. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION

All information which is disclosed by PDAX to the User or by the User to PDAX shall be protected hereunder and considered as Confidential Information.

To the extent that the Parties may disclose information in the course of the performance of the Services, the User may be required to enter into a Confidentiality and Non-Disclosure Agreement with PDAX to ensure compliance with Applicable Laws and Rules, in substantially the following form:

a. Definition of Terms

(i) **Affiliate** refers, in respect of each Party, to such Party's subsidiaries and/or affiliated companies, holding company and its respective subsidiaries and/or affiliated companies, as applicable, existing or coming to exist during the term of this Confidentiality and Non-Disclosure Agreement.

(ii) **Confidential Information** refers to all non-public, confidential or proprietary communications or data, in any form, whether tangible or intangible, which are disclosed or furnished by a Disclosing Party, its Affiliates, and their respective Representatives, to the Receiving Party, its Affiliates, and their respective Representatives, and which are to be protected hereunder against unrestricted disclosure or competitive use by the Receiving Party. The following are also Confidential Information:

- technical information, which refers to methods, processes, formulae, compositions, inventions, machines, computer programs, and research projects; and
- business information, which refers to User lists; pricing data sources of supply; marketing, production, or merchandising systems or plans; and all information or material that has or could have commercial value or other utility in the business of the Disclosing Party.

All information which is disclosed by the Disclosing Party to the Receiving Party and which is to be protected hereunder by the Receiving Party shall be considered as Confidential Information.

Confidential Information excludes:

- information that becomes generally available to the public other than as a result of the disclosure by the Receiving Party in violation of this Confidentiality and Non-Disclosure Agreement;

- information available to a Receiving Party on a non-confidential basis prior to disclosure by the Disclosing Party;
- information made available to the Receiving Party on a non-confidential basis by the Disclosing Party;
- information that is required to be disclosed by any court, tribunal, or regulatory authority or by any requirement of law, legal process, regulation, or governmental order, decree, or rule, or necessary or desirable for a Party to disclose in connection with any proceeding in any court, tribunal or before any regulatory authority in order to preserve its rights;
- information that the Disclosing Party expressly agrees in writing to be disclosed by the Receiving Party to Third Parties;
- information lawfully received from an independent Third Party without any restriction and without any obligation of confidentiality;
- information disclosed without restriction by the Disclosing Party to any Third Party; and
- information which is independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

(iii) **Disclosing Party** refers to the party disclosing Confidential Information.

(iv) **Receiving Party** refers to the party receiving Confidential Information.

(v) **Representatives** refers to any director, officer, employee, agent, or consultant of any department or business area of a Party.

(vi) **Third Party** means any party other than PDAX and the User.

b. **Disclosure of Confidential Information** – The Disclosing Party hereby represents and warrants to the Receiving Party that it has lawful rights to provide the Confidential Information. Confidential Information will be disclosed either:

(i) in writing;

(ii) by delivery of items;

(iii) by initiation of access to Confidential Information, such as may be in a database; or

(iv) by oral or visual presentation.

c. **Restrictions on Use of Confidential Information** – Usage of Confidential Information shall be restricted, as follows:

(i) The Receiving Party agrees, for itself, its Affiliates, and their respective Representatives, to (a) hold all Confidential Information

(regardless of whether it is specifically marked confidential or not) in strict confidence; (b) transmit the Confidential Information only to its Representatives, its Affiliates, and its Affiliates' Representatives, on a 'need-to-know' basis and after each one of them has agreed to be bound by the terms and conditions of this Confidentiality and Non-Disclosure Agreement and not to disclose the same except as provided herein; (c) not to directly or indirectly use, copy, digest, or summarize any Confidential Information except as provided in this Confidentiality and Non-Disclosure Agreement, and (d) not to disclose any Confidential Information to any third party without the prior written consent of the Disclosing Party. In the event that Receiving Party becomes aware that Confidential Information has been disclosed to or accessed by any unauthorized party, the Receiving Party shall immediately notify the Disclosing Party thereof and shall take all appropriate countermeasures.

(ii) The Receiving Party shall strictly comply with any and all Applicable Laws and Rules, including but not limited to the DPA, as well as any policy, measures, rules, and regulations of the Disclosing Party implementing such Applicable Laws and Rules. The Receiving Party understands and agrees that the Disclosing Party shall have no liability for any of the Receiving Party's acts or omissions which may be in violation of such Applicable Laws and Rules as well as the Disclosing Party's rules.

(iii) Likewise, should the Receiving Party need to contract third parties to aid in the fulfillment of the Purpose, the Receiving Party should fully disclose all these third parties and secure written consent from the Disclosing Party prior to any disclosure of Confidential Information.

(iv) The Disclosing Party may grant its consent for the disclosure of the Confidential Information in its sole discretion and on a case-to-case basis. The Receiving Party expressly agrees not to use the Confidential Information to gain or attempt to gain a competitive advantage over the Disclosing Party.

(v) If requested by the Disclosing Party, the Receiving Party shall acknowledge receipt of any Confidential Information by signing receipts, initialing documents, or any other means that the Disclosing Party may reasonably request.

(vi) The Receiving Party will not permit copies of the Confidential Information to be made without the express written consent of the Disclosing Party. Copies shall be deemed confidential and, in all respects, subject to the terms of this Confidentiality and Non-Disclosure Agreement.

(vii) If the Receiving Party is requested by a governmental entity to disclose any Confidential Information, it will promptly notify the Disclosing Party to allow the Receiving Party to do so. The Receiving Party will also cooperate in the Disclosing Party's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be afforded the Confidential Information. If in the absence of a protective order and the Receiving Party is compelled as a matter of law to disclose the Confidential Information, based upon the written opinion of the Receiving Party addressed to the Disclosing Party, the Receiving Party may disclose to the Party compelling the disclosure only the part of the Confidential Information as required by law to be disclosed. The Receiving Party will advise and consult with the Disclosing Party as to such disclosure and the nature and wording of such disclosure and the Receiving Party will use its best efforts to obtain confidential treatment therefore.

d. **No Publicity** – Either Party shall not, in any way or in any form, disclose, publicize, or advertise in any manner the definitive agreements executed between the Parties, including this Confidentiality and Non-Disclosure Agreement, and the discussions or negotiations they cover and their execution, except through a notarial act, or through the prior written consent of the other Party.

e. **Property Rights and Ownership** – All Confidential Information, unless otherwise specified in writing, shall remain the sole and exclusive property of the Disclosing Party and shall be used by the Receiving Party only in furtherance of the Service, except as may be required by applicable law or legal process.

Each Party retains ownership, including intellectual property rights, over all preexisting materials, documents and work originally created by them and independently developed and contributed towards the implementation of the Service. The ownership over any materials, documents and work resulting from undertaking the Service and created in collaboration with and through the joint efforts of the Parties shall be subject to the terms of definitive agreements to be negotiated by the Parties.

No other rights, and particularly no license and no assignment of intellectual property rights including copyright, patent rights, design rights, trademarks, and mask work protection rights are implied or

granted under this Confidentiality and Non-Disclosure Agreement. The Parties shall not make use of the existence of any bilateral business relationship between them for the purpose of their own advertisement.

f. **Safekeeping** – The Receiving Party shall use the same care to avoid disclosure or unauthorized use of the Confidential Information as it uses to protect its own Confidential Information, but in no event less than reasonable care. It is agreed that:

(i) All Confidential Information shall be retained by the Receiving Party in a secure place with access limited only to the Receiving Party's Representatives who need to know such information for purposes of this Confidentiality and Non-Disclosure Agreement; and

(ii) Confidential Information will be disclosed only to each Party's Representatives who are involved in the performance of the Service. It may be disclosed to third party consultants or advisers for the purpose of discussing the Service, only with the prior consent of the Disclosing Party. In the event of such disclosure to any third party, the Receiving Party shall remain liable for any unauthorized disclosure by such person or entity.

(iii) The Receiving Party shall ensure that all of its Representatives, Affiliates, and Representatives of Affiliates, and third-party consultants having access to Confidential Information adhere to the terms and conditions of this Confidentiality and Non-Disclosure Agreement as if they were Parties hereto.

g. **Return of Confidential Information** – All Confidential Information, including but not limited to copies, summaries, excerpts, extracts, drawings, blueprints, reports, manuals, correspondence, User lists, computer programs, and all other materials and all hard, soft, manual, paper, and electronic copies of such Confidential Information or any and all documents or materials relating in any way to the Disclosing Party's business or to a Data Subject, or any documents or materials in any way disclosed, obtained, or accessed during the course of the relationship between the Parties, or other reproduction thereof, shall be returned to the Disclosing Party upon the termination of this Confidentiality and Non-Disclosure Agreement.

In addition, the Receiving Party shall return to the Disclosing Party all copies of written, taped, or audio-visual recorded Confidential Information, which consists of analysis, compilation, forecasts, studies, or other documents, in its possession and promises not to retain any such copies.

h. **Provisional Remedy for Potential Breach** – The Parties recognize that money damages may not be a sufficient remedy for any breach of the foregoing covenants and agreements, and that any such breach may cause grave and irreparable injury to the other party. The Disclosing Party shall be entitled to specific performance, and injunctive and other equitable relief against the other party in respect of the threatened breach of this Confidentiality and Non-Disclosure Agreement or the continuation of any such breach, in addition to all monetary or other remedies available at law or in equity.

i. **Term** – This Confidentiality and Non-Disclosure Agreement shall be co-terminous with, and shall be terminated in accordance with, the Terms and Conditions and the Remittance Rules, save the obligation of maintaining confidentiality.