DATA SHARING AGREEMENT FOR i2i

I. User Agreement

This document sets out the Data Sharing Agreement that will govern the use of i2i and its products. This embodies the agreement between the Member and **UBX Philippines Corporation ("UBX PH"),** operator of i2i.

By accessing, browsing and/or using the Platform, you acknowledge that you have read, understood, and agree to be bound by this Data Sharing Agreement and to comply with all applicable laws and regulations relative to your use of the Platform.

II. About i2i

i2i is a platform that utilizes blockchain technology. It enables its member institutions to connect with one another to conduct transactions with each other or with other networks (i.e., Pesonet, Instapay). The platform is available via web. Various financial or non-financial products and services (collectively termed as **"Products"**) shall be offered in the i2i platform to its various members. Acceptance of the i2i platform does not automatically grant a member the right to avail of its products. Each product shall have its own separate Service Agreement that will govern the specific conditions of that product.

III. Definition of Terms

1. **Consent of the Data Subject** refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

2. **Data Exporter** shall mean the controller who transfers the personal data.

3. **Data Importer** shall mean the controller who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of this Agreement.

4. **Data Privacy Act ("DPA")** shall pertain to Republic Act No. 10173, its amendments and its implementing rules and regulations, as may be revised and other related issuances of the National Privacy Commission (NPC).

5. **Data Subject** refers to: (i) an individual whose personal, sensitive personal, or privileged information is processed; (ii) an individual who is an account holder or member, who has provided his or her information to the Parties, who has provided his or her information in the Parties' website; and (iii) upon his or her consent, such information shall be shared by Data Exporter with Data Importer for the purpose of this Agreement. With respect to the Platform, the sender and the receiver shall be referred to as Data Subjects.

6. **Data Processing** refers to any operation or any set of operations performed upon Personal Information 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 information is contained or are intended to be contained in a filing system.

7. **Member** pertains to a duly organized and existing entity that is onboarded in i2i, transacts in i2i or has availed of any of i2i's Products.

8. **Personal Data** shall refer collectively to the Personal Information and Sensitive Personal Information.

9. **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.

10. **Personal Information Controller ("PIC")** refers to the Parties of this Agreement, both of which control the processing of Personal Information or instructs another party to process Personal Information on its behalf.

11. **Personal Information Processor ("PIP")** refers to any natural or juridical person or any other body to whom PIC may outsource or instruct the processing of personal information pertaining to a data subject.

12. **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 information transmitted, stored, or otherwise processed. It shall also refer to (a) any act or omission that compromises or may compromise either the security, confidentiality or integrity of the Data Subject's Personal Information, or the physical, technical, administrative or organizational safeguards put in place by the Parties that relate to the protection of the security, confidentiality or integrity of Data Subject's Personal Information, or (b) receipt of a complaint in relation to the privacy practices of the Parties or a breach or alleged breach of this Agreement relating to privacy practices.

13. **Sensitive Personal Information** refers to personal information (a) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (b) 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings; (c) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (d) Specifically established by an executive order or an act of Congress to be kept classified.

IV. Principles

1. Each Party recognizes that the Data Subject or the Customer, whether a sender or a receiver, inevitably needs to disclose his or her Personal Data to both Parties and all parties in the Platform for the transaction to push through.

2. All right, title, and interest in the Personal Data of Data Subjects who consented that their personal information be shared with Data Importer, shall be co-controlled by the Parties.

3. This Agreement may be subject to review by the NPC as provided under the DPA. As such, the Parties agree to exert best efforts and good faith in ensuring that the Agreement and its operationalization reflect any revisions or required provisions that may be required by the NPC pursuant to said review.

4. All Parties may be the Data Exporter and the Data Importer, as the case may be.

V. Security Obligations

Pursuant to its obligation to maintain the appropriate technical, physical, and organizational security measures, the each Party warrants that, at minimum, it shall have the following security measures:

1. Organizational Security Measures

a. That it has a designated individual who functions as data protection officer.

b. That it has implemented appropriate data protection policies that provide for organization, physical and technical security measures, 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 subject.

c. The policies shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.

2. Physical Security Measures

a. 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.

b. That the design of its office space and work stations shall provide privacy to anyone processing Personal Data, taking into consideration the environment and accessibility to the public.

3. Technical Security Measures

a. 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.

b. That it has the ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services.

c. 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.

d. 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.

VI. Obligations for Data Privacy and Security

1. The Member shall at all times be responsible for ensuring that the Personal Data, in whatever form, is stored securely. The Member hereby agrees to implement security measures to maintain the confidentiality, integrity, and availability of the Personal Data; and protect it from accidental or unlawful destruction, alteration and unauthorized disclosure, unlawful processing or use, fraudulent misuse, or loss or destruction while in the Member's custody or its subcontractor.

2. The Member shall maintain, and periodically review and update when necessary its data protection and security policies with respect to the processing of the Personal Data and its processes on identifying vulnerabilities in its computer networks, as well as the procedure for prevention, mitigation and correction of security incidents that may lead to security breaches, to ensure continuous compliance with the DPA, and all applicable data privacy rules and regulations.

3. The Member agrees that its personnel, agents, representatives or any other person under its control or authority, shall have access to the Personal Data only as legitimate purpose and proportionality would require, with purpose being only the implementation of this Agreement, and will store and/or process the Personal Data in accordance with the DPA, and relevant data privacy regulations.

4. In case of any judicial order, governmental action, or legal obligation requiring the Member to disclose Personal Data, the Member shall immediately inform UBX PH, but in no case later than twenty-four (24) hours from knowledge thereof. The Member shall at the first instance possible, raise the confidential nature of the required information and in all cases exert the necessary efforts in legally resisting said disclosure and any disclosure shall not be in excess of the information required by the order.

5. The Processing of Customer Data shall be made only in accordance with this Agreement or, subject to the notice requirements set herein, as required by law or regulatory mandate.

6. The Data Exporter, on its own or through its employees, agents, personnel, or representatives, shall obtain the Consent of the Data Subject before the disclosure of Personal Data to the Data Importer.

7. The Data Importer, on its own or through its employees, agents, personnel, or representatives, shall limit the processing of Personal Data with respect to the product that the Member has availed or subscribed to in i2i.

VII. Personal Data Breach Management and Reporting Obligation

1. If the Member suspects or becomes aware of any security breach or potential security breach involving Personal Data of Data Subjects within its network, operating systems, software applications, data storage systems, media channels or other office procedures, the Member shall notify UBX PH in writing within twenty-four (24) hours from the occurrence or discovery of the breach and shall fully cooperate with UBX PH, to prevent or stop the Personal Data Breach.

2. The Member shall defend, indemnify, and hold UBX PH, its subsidiaries, affiliates, and their respective officers, directors, stockholders, employees, and agents free and harmless from and against any and all claims, suits, causes of action, liability, loss, costs, and damages, including attorney's fees and costs of litigation, in connection with or as a result of any third party claim arising from the Personal Data Breach of the Member.

3. In case the Personal Data Breach is material and substantial, and such will cause UBX PH irreparable injury for which it would have no adequate remedy at law and for which there is an urgent and permanent necessity to prevent serious damage, UBX PH shall be entitled to immediately seek injunctive relief against all relevant parties in addition to any other rights and remedies available to it under law or this Agreement.

4. Immediately following the notification of a Personal Data Breach sent by the Member to UBX PH, the parties shall coordinate with each other to investigate said breach. Each party agrees to fully cooperate with the other and provide a root cause analysis report within reasonable time, which unless a shorter time is required by relevant law and/or the NPC, should be not later than twenty-four (24) hours from the discovery of the breach.

5. The Member shall immediately remedy any Personal Data Breach and prevent any such breach at the Member's sole expense in accordance with the DPA and all relevant international standards on data protection. The Member shall also reimburse UBX PH for actual costs incurred by UBX PH in responding to and mitigating damages caused by the Personal Data breach.

6. The Member agrees that it shall not inform any third party of any Personal Data Breach affecting UBX PH without first notifying UBX PH and UBX PH agreeing to the disclosure. Both parties shall work together in drafting the contents of any such notice prior to submission to the relevant authorities. In the

event of any Personal Data breach, Member shall ensure that all measures and safeguards to prevent a recurrence of any such Personal Data Breach are immediately put in place.

VIII. Confidentiality and Non-Disclosure Clause

1. All information or data acquired in connection with this Agreement, the Terms and Conditions on the use of i2i, other documents pertaining to the subscribed or availed product of i2i or in relation to the Parties' respective obligations herein, including the Personal Data, shall be treated by it, its representatives, officers, employees, subcontractors and any other person that may be utilized by said Party, as strictly confidential ("Confidential Information") and shall not at any time be disclosed or caused to be disclosed to any person, except with the prior written consent of the other.

2. All Parties shall (a) use such Confidential Information for the sole and limited purpose of complying with its respective obligations under this Agreement; (b) not copy, in whole or in part, Confidential Information without the other Party's prior express written consent; (c) return all Confidential Information, including copies or other written or physical embodiments of, or containing, such Confidential Information (including any studies, analyses, compilations or other materials prepared in whole or in part based on said Confidential Information) to the Data Exporter immediately upon the written or oral request of said Data Exporter, or upon termination of this Agreement, whichever occurs first.

3. Neither Party shall, without the prior consent of the other, disclose or make available to any person, make public, or use directly or indirectly, except for the performance and implementation of the Program, any confidential information acquired from Data Exporter or information holder in connection with the performance of its obligations under this Agreement, except for the following:

   a. When an information is known to the Data Exporter, as evidenced by its written records, prior to obtaining the same from its holder and is not otherwise subject to disclosure restrictions on the Data Exporter;
   b. When the information is disclosed to the Data Exporter by a third party who did not receive the same, directly or indirectly, from an information holder, and who has no obligation of secrecy with respect thereto; or
   c. When the information is required to be disclosed by law.

4. Each Party shall use the same degree of care to maintain the confidentiality of the Confidential Information as it uses with respect to its own confidential information, but in no event less than a reasonable degree of care.

5. Except as otherwise provided herein, the obligations of the Parties herein shall remain effective and continue in full force for the duration of this Agreement and shall survive for a period of two (2) years from the termination thereof.

6. Where necessary, required, or beneficial for the validity or enforceability of this Agreement, nothing contained herein shall be construed as to prevent the Parties from registering or otherwise submitting this Agreement to the appropriate government office or regulatory agency.

7. This shall be inoperative as to particular portions of the Confidential Information to the extent such information:

   a. Becomes generally available to the public other than as a result of a disclosure by any of the Parties, or any Affiliates or Representatives;
   b. Was available to the Parties on a non-confidential basis prior to its disclosure;
   c. Was created independently by a Party without using the Confidential Information provided by another Party;

d. Was authorized by the Disclosing Party to be shared with a third party.

IX. Privacy Notice

In compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and issuances by the NPC, the Member shall ensure that the following PRIVACY NOTICE is conspicuously and publicly available for Data Subject's visibility. The same may be printed and posted on conspicuous bulletin boards, posted on the online platform, or visible together with the forms Data Subjects are required by law to accomplish.

PRIVACY NOTICE

We take the privacy and protection of your Personal Data seriously. As end-user of the i2i Platform, whether as sender or receiver, you are referred to as Data Subjects of both _____ [full registered name of Member] and UBX PH, who have vested privacy rights under the Data Privacy Act of 2012. We collect the following Personal Data about you: name, date of birth, place of birth, civil status, nationality, address, mobile number, landline, number, email address, bank account details, occupation, name of employer, source of funds, amount, purpose, and other details as may be required by the nature of your transaction. To know more about our Privacy Policy, please go to this site: _____[URL of i2i]. For questions, requests, and notifications, communication may be directed to _____ [full registered name of Member].

X. Personal Data Inventory

The Products of i2i shall require one or a combination of some or all of the personal information attributes enumerated below from its Member's customers.

Personal Information Attribute	Category
Customer's First Name	Personal Information
Customer's Middle Name	Personal Information
Customer's Last Name	Personal Information
Customer's Address	Personal Information
Gender	Sensitive
Mobile Number	Personal Information
Customer's Bank	Personal Information
Customer's Account Number	Sensitive
Amount	Sensitive
Purpose of Transaction	Non-Personal
Other details as may be required	--