Data Processing Addendum

Current as of January 31, 2024

This Data Processing Addendum (this “**Addendum**”) is incorporated into the Agreement between Libum and Customer. Capitalized terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Agreement.

The parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. The following obligations shall only apply to the extent required by Data Protection Laws with regard to the relevant Customer Personal Data, if applicable.

1. Definitions

“**Controller**” means an entity that determines the purposes and means of the Processing of Personal Data.

“**Customer Personal Data**” means Personal Data Processed by Libum on behalf of Customer to perform the Services under the Agreement.

“**Data Protection Laws**” means the data privacy and security laws and regulations of any jurisdiction applicable to the Processing of Customer Personal Data, including: (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (collectively, “**CCPA**”); (b) the Virginia Consumer Data Protection Act (“**VCPDA**”); (c) the Colorado Privacy Act and its implementing regulations (“**CPA**”), when effective; (d) the Utah Consumer Privacy Act (“**UCPA**”), when effective; and (e) the Connecticut Data Privacy Act (“**CTDPA**”), when effective.

“**Data Subject**” means the identified or identifiable natural person who is the subject of Personal Data.

“**Personal Data**” means information that constitutes “personal information,” “personal data,” “personally identifiable information,” or similar term under Data Protection Laws.

“**Process**” means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, alignment, combination, restriction, erasure, destruction or disclosure by transmission, dissemination or otherwise making available.

“**Processor**” means an entity that Processes Personal Data on behalf of a Controller.

“**Security Incident**” means a breach of Libum’s security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data in Libum’s possession, custody, or control. “Security Incident” does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

“**Services**” means the services that Libum has agreed to provide to Customer under the Agreement.

“**Subprocessor**” means any Processor appointed by Libum to Process Customer Personal Data on behalf of Customer under the Agreement.

2. Processing of Customer Personal Data

2.1 Roles of the Parties; Compliance.

The parties acknowledge and agree that, as between the parties, with regard to the Processing of Customer Personal Data under the Agreement, Customer is a Controller and Libum is a Processor. In some circumstances, the parties acknowledge that Customer may be acting as a Processor to a third-party Controller in respect of Customer Personal Data, in which case Libum will remain a Processor with respect to the Customer in such event. Each party will comply with the obligations applicable to it in such role under Data Protection Laws with respect to the Processing of Customer Personal Data.

2.2 Customer Instructions

Libum will Process Customer Personal Data only in accordance with Customer's documented instructions unless otherwise required by applicable law, in which case Libum will inform Customer of such Processing unless notification is prohibited by applicable law. Customer hereby instructs Libum to Process Customer Personal Data: (a) to provide the Services to Customer; (b) to perform its obligations and exercise its rights under the Agreement and this Addendum; and (c) as necessary to prevent or address technical problems with the Services. Libum will notify Customer if, in its opinion, an instruction of Customer infringes upon Data Protection Laws. Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws. Customer shall be responsible for: (i) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and Libum's Processing of Customer Personal Data; and (ii) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to Libum to permit the Processing of such Customer Personal Data by Libum for the purposes of performing Libum's obligations under the Agreement or as may be required by Data Protection Laws. Customer shall notify Libum of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Customer Personal Data that would impact Libum's ability to comply with the Agreement, this Addendum, or Data Protection Laws.

2.3 Details of Processing

The parties acknowledge and agree that the nature and purpose of the Processing of Customer Personal Data, the types of Customer Personal Data Processed, the categories of Data Subjects, and other details regarding the Processing of Customer Personal Data are as set forth in Appendix 1.

2.4 Processing Subject to the CCPA

As used in this Section 2.4, the terms "Sell," "Share," "Business Purpose," and "Commercial Purpose" shall have the meanings given in the CCPA and "Personal Information" shall mean any personal information (as defined in the CCPA) contained in Customer Personal Data. Libum will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Agreement, including for any Commercial Purpose other than the Business Purposes specified in the Agreement, or as otherwise permitted by the CCPA, or (ii) outside of the direct business relationship between Customer and Libum; or (c) combine Personal Information received from, or on behalf of, Customer with Personal Data received from or on behalf of any third party, or collected from Libum's own interaction with Data Subjects, except to perform any Business Purpose permitted by the CCPA. Libum hereby certifies that it understands the foregoing restrictions under this Section 2.4 and will comply with them. The parties acknowledge that the Personal Information disclosed by Customer to Libum is provided to Libum only for the limited and specified purposes set forth in Appendix 1. Libum will comply with applicable obligations under the CCPA and provide the same level of privacy protection to Personal Information as is required by the CCPA. Customer has the right to take reasonable and appropriate steps to help ensure that Libum uses the Personal Information transferred in a manner consistent with Customer's obligations under the CCPA by exercising Customer's audit rights in Section 8. Libum will notify Customer if it makes a determination that Libum can no longer meet its obligations under the CCPA. If Libum notifies Customer of unauthorized use of Personal Information, including under the foregoing sentence, Customer will have the right to take reasonable and appropriate steps to stop and remediate such unauthorized use by limiting the Personal Information shared with

Libum, terminating the portion of the Agreement relevant to such unauthorized use, or such other steps mutually agreed between the parties in writing.

3. Confidentiality

Libum shall take reasonable steps to ensure that Libum personnel who Process Customer Personal Data are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality with respect to such Customer Personal Data.

4. Security

4.1 Security Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Libum shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, in accordance with the security standards in Appendix 2 (the "**Security Measures**"). Customer acknowledges that the Security Measures may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices, provided that the modifications will not materially decrease Libum's security obligations hereunder.

4.2 Security Incidents

Upon becoming aware of a confirmed Security Incident, Libum will: (a) notify Customer of the Security Incident without undue delay after becoming aware of the Security Incident; and (b) take reasonable steps to identify the cause of such Security Incident, minimize harm, and prevent a recurrence. Libum will take reasonable steps to provide Customer with information available to Libum that Customer may reasonably require to comply with its obligations under Data Protection Laws. Libum's notification of or response to a Security Incident under this Section 4.2 will not be construed as an acknowledgement by Libum of any fault or liability with respect to the Security Incident.

4.3 Customer Responsibilities

Customer agrees that, without limitation of Libum's obligations under this Section 4, Customer is solely responsible for its use of the Services, including: (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; and (b) securing any account authentication credentials, systems, and devices Customer uses to access or connect to the Services, where applicable. Without limiting Libum's obligations hereunder, Customer is responsible for reviewing the information made available by Libum relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

5. Subprocessing

Subject to the requirements of this Section 5, Customer generally authorizes Libum to engage Subprocessors as Libum considers reasonably appropriate for the Processing of Customer Personal Data. A list of Libum's Subprocessors, including their functions and locations, is available upon Customer's request and may be updated by Libum from time to time in accordance with this Section 5. Libum will notify Customer of the addition or replacement of any Subprocessor at least ten (10) days prior to such engagement. Customer may object to such changes on reasonable data protection grounds by providing Libum written notice of such objection within ten (10) days. Upon receiving such an objection, where practicable and at Libum's sole discretion Libum will use commercially reasonable efforts to: (a) work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; or (b) take corrective steps requested by Customer in its objection and proceed to use the new Subprocessor. If Libum informs Customer that such change or corrective steps cannot be made, Customer may, as its sole and exclusive remedy available under this Section 5, terminate the relevant portion of the Agreement involving the Services which require the use of the proposed Subprocessor by providing written notice to Libum. When engaging any Subprocessor, Libum will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this Addendum. Libum shall be liable for the acts and omissions of the Subprocessor to the extent Libum would be liable under the Agreement and this Addendum.

6. Data Subject Rights

Libum will, taking into account the nature of the Processing of Customer Personal Data and the functionality of the Services, provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, as necessary for Customer to fulfill its obligations under Data Protection Laws to respond to requests by Data Subjects to exercise their rights under Data Protection Laws. Libum reserves the right to charge Customer on a time and materials basis in the event that Libum considers that such assistance is onerous, complex, frequent, or time consuming. If Libum receives a request from a Data Subject under any Data Protection Laws with respect to Customer Personal Data, Libum will advise the Data Subject to submit the request to Customer and Customer will be responsible for responding to any such request.

7. Assessments and Prior Consultations

In the event that Data Protection Laws require Customer to conduct a data protection impact assessment, transfer impact assessment, or prior consultation with a regulatory authority in connection with Libum's Processing of Customer Personal Data, following written request from Customer, Libum shall use reasonable commercial efforts to provide relevant information and assistance to Customer to fulfill such request, taking into account the nature of Libum's Processing of Customer Personal Data and the information available to Libum. Libum reserves the right to charge Customer on a time and materials basis in the event that Libum considers that such assistance is onerous, complex, frequent, or time consuming.

8. Relevant Records and Audit Rights

8.1 Review of Information and Records

Upon Customer's reasonable written request, Libum will make available to Customer all information in Libum's possession reasonably necessary to demonstrate Libum's compliance with Data Protection Laws and Libum's obligations set out in this Addendum. Such information will be made available to Customer no more than once per calendar year and subject to the confidentiality obligations of the Agreement or a mutually-agreed non-disclosure agreement.

8.2 Audits

If Customer requires information for its compliance with Data Protection Laws in addition to the information provided under Section 8.1, at Customer's sole expense and to the extent Customer is unable to access the additional information on its own, Libum will allow for, cooperate with, and contribute to reasonable assessments and audits, including inspections, by Customer or an auditor mandated by Customer ("**Mandated Auditor**"), provided that (a) Customer provides Libum with reasonable advance written notice including the anticipated date of the audit, the proposed scope of the audit, and the identity of any Mandated Auditor, which shall not be a competitor of Libum; (b) Libum approves the Mandated Auditor in writing, with such approval not to be unreasonably withheld; (c) the audit is conducted during normal business hours and in a manner that does not have any adverse impact on Libum's normal business operations; (d) Customer or any Mandated Auditor complies with Libum's standard safety, confidentiality, and security policies or procedures in conducting any such audits; (e) any records, data, or information accessed by Customer or any Mandated Auditor in the performance of any such audit, or any results of any such audit, will be deemed to be the Confidential Information of Libum and subject to a nondisclosure agreement to be provided by Libum; and (f) Customer may initiate such audit not more than once per calendar year unless otherwise required by a regulatory authority or Data Protection Laws.

8.3 Results of Audits

Customer will promptly notify Libum of any non-compliance discovered during the course of an audit and provide Libum any reports generated in connection with any audit under this Section, unless prohibited by Data Protection Laws or otherwise instructed by a regulatory authority. Customer may use the audit reports solely for the purposes of meeting Customer's audit requirements under Data Protection Laws to confirm that Libum's Processing of Customer Personal Data complies with this Addendum.

9. Data Transfers

During the term of the Addendum, Customer Personal Data shall at all times be hosted on servers that are physically located in the United States, unless otherwise agreed in writing by the parties. Libum shall comply, and provide Customer with commercially reasonable assistance to comply, with all applicable cross-border transfer laws, regulations, and guidelines in the country to which and from which Customer Personal Data will be transferred. Libum shall legitimize any cross-border exchange of Customer Personal Data through data transfers mechanisms approved under Data Protection Laws, such as United Kingdom- or Europe Union-approved standard contractual clauses or EU-U.S. Data Privacy Framework with respect to transfers of Personal Data out of the United Kingdom or Europe Union.

10. Deletion or Return of Customer Personal Data

Following termination or expiration of the Agreement, Libum shall, at Customer's option, delete or return Customer Personal Data and all copies to Customer, except as required by applicable law. If Libum retains Customer Personal Data pursuant to applicable law, Libum agrees that all such Customer Personal Data will continue to be protected in accordance with this Addendum.

11. General Terms

This Addendum will, notwithstanding the expiration or termination of the Agreement, remain in effect until, and automatically expire upon, Libum's deletion or return of all Customer Personal Data. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible; or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. To the extent of any conflict or inconsistency between this Addendum and the other terms of the Agreement in relation to the Processing of Customer Personal Data, this Addendum will govern. Unless otherwise expressly stated herein, the parties will provide notices under this Addendum in accordance with the Agreement, provided that all such notices may be sent via email. Any liabilities arising in respect of this Addendum are subject to the limitations of liability under the Agreement. This Addendum will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

Appendix 1: Details of Processing of Customer Personal Data

Current as of January 31, 2024

1. Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing are as described in the Agreement and the Addendum.

2. Nature and purpose of the Processing of Customer Personal Data

The nature and purpose of the Processing are those activities reasonably required to facilitate or support the provision of the Services as described in the Agreement and the Addendum.

The purpose of the Processing of Customer Personal Data includes the following:

- Helping to ensure security and integrity, to the extent the use of Customer Personal Data is reasonably necessary and proportionate for these purposes;
- Debugging to identify and repair errors that impair existing intended functionality;
- Short-term, transient use, specifically for credit union operations;
- Performing the Services as described in the Agreement and carrying out the instructions set forth in Section 2.2, including providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of Customer;
- Undertaking internal research for technological development and demonstration; and
- Undertaking activities to verify or maintain the quality or safety of the Services, and to improve, upgrade, or enhance the Services.

3. *The categories of Data Subjects to whom Customer Personal Data relates*

The categories of Data Subjects shall be as is contemplated or related to the Processing described in the Agreement.

4. *The categories of Customer Personal Data*

The categories of Customer Personal Data Processed are those categories contemplated in and permitted by Agreement.

5. *The sensitive data included in Customer Personal Data*

Any sensitive information contained in the Customer Personal Data shall be secured in accordance with the safeguards described in Appendix 2 and any additional safeguards required by Data Protection Laws applicable to such sensitive information.

6. *The frequency of Customer's transfer of Customer Personal Data to Service Provider:*

On a continuous basis for the term of the Agreement.

7. *The period for which Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:*

As set forth in the Addendum or the Agreement.

Appendix 2: Security Measures

Current as of January 31, 2024

1. Information Security Program

Implement, maintain, and comply with information security policies and procedures designed to protect the confidentiality, integrity, and availability of Customer Personal Data and any systems that store or otherwise Process it, which are: (a) aligned with an industry-standard control framework (e.g., NIST SP 800-53, ISO 27001, CIS Critical Security Controls); (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Customer Personal Data.

2. Risk Assessment

Maintain risk assessment procedures for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance with the organization's policies and procedures, and reporting the condition of the organization's information security and compliance to internal senior management.

3. Personnel Training

Train personnel to maintain the confidentiality, integrity, and availability of Customer Personal Data, consistent with the terms of the Agreement and Data Protection Laws.

4. Vendor Management

Prior to engaging Subprocessors and other subcontractors, conduct reasonable due diligence and monitoring to ensure subcontractors are capable of maintaining the confidentiality, integrity, and availability of Customer Personal Data.

5. Access Controls

Only authorized personnel and third parties are permitted to access Customer Personal Data. Maintain logical access controls designed to limit access to Customer Personal Data and relevant information systems (e.g., granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking or changing access when employment terminates or changes in job functions occur).

6. Secure User Authentication

Maintain password controls designed to manage and control password strength, expiration, and usage. These controls include prohibiting users from sharing passwords and requiring that passwords controlling access to Customer Personal Data must: (a) be at least 8 characters in length and meet minimum complexity requirements; (b) not be stored in readable format on the organization's computer systems; (c) have a history threshold to prevent reuse of recent passwords; and (d) if newly issued, be changed after first use.

7. Incident Detection and Response

Maintain policies and procedures to detect and respond to actual or reasonably suspected Security Incidents, and encourage the reporting of such incidents.

8. Encryption

Apply industry standard encryption to Customer Personal Data: (a) stored on any medium (i.e., laptops, mobile devices, portable storage devices, file servers and application databases); and (b) transmitted across any public network (such as the Internet) or wirelessly.

9. Network Security

Implement network security controls such as up-to-date firewalls, layered DMZs, updated intrusion detection and prevention systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

10. Vulnerability Management

Detect, assess, mitigate, remove, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code, by implementing vulnerability management, threat protection technologies, and scheduled monitoring procedures.

11. Change Control

Follow change management procedures and implement tracking mechanisms designed to test, approve, and monitor all changes to the organization's technology and information assets.

12. Physical Security

Take steps to ensure the physical and environmental security of data centers, server room facilities and other areas containing Customer Personal Data, including by: (a) protecting information assets from unauthorized physical access; (b) managing, monitoring, and logging movement of persons into and out of the organization's facilities; and (c) guarding against environmental hazards such as heat, fire, and water damage.

13. Business Continuity and Disaster Recovery

Maintain business continuity and disaster recovery policies and procedures designed to maintain service and recover from foreseeable emergency situations or disasters.