Addendum 1 to Agreement
Data Processing

This Addendum on Data Processing (hereinafter: "Addendum") is made on the Effective Date, by and between:

Customer as defined by the SOW

– hereinafter referred to as "**Controller**" –
and
Merrill Communication LLC
One Merrill Circle
St. Paul, MN 55108
United States

– hereinafter referred to as "**Processor**" –
Hereinafter each individually referred to also as the "**Party**" and collectively as the "**Parties**"

Preamble:
(A) The Parties have entered into a Statement of Work and General Terms and Conditions ("the Agreement") which outlines the Services to be provided (definitions provided in Section 1 below). As part of the provision of Services by the Processor, Personal Data may be transferred by the Controller to the Processor.

(B) This addendum shall be executed between the Controller and any entity of the Processor and/or any third party retained by the Processor in connection with the Agreement which processes Personal Data on behalf of such entity located in a Data Protection Country.

(C) To ensure compliance by the Controller with Processing obligations pursuant to the Data Protection Rules, as amended from time to time, the Parties hereby agree and covenant as follows:

1. Definitions

1.1. "**Adequate Countries**" means those jurisdictions identified by the European Commission from time to time as providing adequate data protection under Article 45 of the General Data Protection Regulations;

1.2. "**Affiliates**" means all affiliated entities, including any parent, sister, daughter or subsidiary companies, of the Controller or Processor;

1.3. "**Appendix**" or "**Appendices**" means the appendix or appendices annexed to and forming an integral part of this Addendum;

1.4. "**Data Protection Country**" or "Data Protection Countries" means a country or countries (respectively) where privacy, data protection or information security laws are in place that regulate personal or private information or Personal Data, including but not limited to the European Economic Area and Switzerland.

1.5. "**Data Protection Rules**" means the relevant national laws that apply to the Processing of Personal Data in Data Protection Countries, including but not limited to any applicable privacy and information security laws and regulations that apply from time to time;

1.6. "**Data Subject**" means an identified or identifiable natural person whose Personal Data is subject to Processing; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity;

1.7. "**General Data Protection Regulations**" means the Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on "the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data" as amended or replaced from time to time;

1.8. "**Information Security Incident**" means any transfer, access and disclosure to third parties, or Processing in breach of this Addendum or the Data Protection Rules or any event directly or indirectly affecting the confidentiality, integrity, authenticity of Personal Data;

1.9. "**Instruction(s**)" has the same meaning given to that expression in Section 4.1 of this Addendum;

1.10. "**Privacy Shield Frameworks**" means the EU-U.S. Privacy Shield Framework, which became effective August 1, 2016, and Swiss-U.S Privacy Shield Framework, which became effective April 12, 2017.

1.11. **"Agreement**" means the Statement of Work and the General Terms and Conditions between the Controller and the Processor;

1.12. "**Personal Data**" means any information relating to a Data Subject;

1.13. "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

1.14. "**Services**" means the Processing by the Processor in connection with and for the purposes of the provision of the services to be provided by the Processor to the Controller under the Agreement;

1.15. "**Special Categories of Data**" means the Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data that uniquely identify a natural person, as well as Personal Data concerning health, sex life or sexual orientation.

2. Subject Matter and Purpose of this Addendum

The Controller warrants that it will only provide Personal Data that is authorized for a permitted purpose to the Processor and the Controller is responsible for ensuring Controller's invitees are aware of their obligations to protect Personal Data that is made available to them for a permitted purpose. The Processor shall Process, on behalf of the Controller, the Personal Data only within the scope and for the purposes detailed in Appendix 1 of this Addendum. This Addendum is intended to ensure adequate protection of Personal Data and information security and does not otherwise

affect the rights and obligations between Parties under other agreements. In the event of any conflict between the provisions in this Addendum and the provisions set forth in the Agreement, the provision or provisions of this Addendum will prevail.

3. Duration and Termination of this Addendum

3.1. This Addendum is effective as of the Effective Date and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of the final SOW.

3.2. Notwithstanding the termination of this Addendum, the Processor and any subcontractors (pursuant to Sections 6.1 and 9 of this Addendum) shall continue to be bound by their obligations of confidentiality.

4. Instructions of the Controller

4.1. The Processor will Process the Personal Data provided by the Controller solely in accordance with the Controller's written instructions and the provisions contained in this Addendum and its Appendices and as may be communicated by the Controller from time to time ("Instructions"). The current Addendum constitutes written instructions.

4.2. If the Processor believes that an Instruction infringes applicable Data Protection Rules, it will immediately notify the Controller.

5. General Obligations of the Processor

5.1. The Processor undertakes to Process the Personal Data in accordance with applicable Data Protection Rules; specifically, with respect to Personal Data from the European Economic Area or Switzerland, in accordance with its obligations as a data processor under its Privacy Shield certification. The Processor undertakes that it will Process the Controller's Personal Data on behalf of the Controller and only in compliance with its Instructions, as described in Appendix 1, and under the provisions of this Addendum. The Processor will also inform the Controller about any relevant changes concerning the Processing of its Personal Data.

5.2. The Processor will neither transfer nor communicate the Personal Data to third parties nor Process or use it for its own purposes, unless otherwise stipulated in this Addendum and in accordance with the Data Protection Rules. The Processor may transfer Personal Data to its wholly owned affiliates for Processing for specialized Services or localization of customer support. The Processor will only onward transfer Personal Data in strict compliance with the Data Protection Rules and the requirements of the Privacy Shield and upon the prior written approval of the Controller.

5.3. The Processor is not allowed to make copies or duplicates of the Personal Data without the prior written consent of the Controller, unless such copies or duplicates are necessary for the fulfillment of its obligations under this Addendum or the Agreement.

5.4. The Processor will not obtain any rights or title to any Personal Data by virtue of providing the Services, and may not determine the purposes for which Personal Data it receives under the Addendum may be Processed or otherwise used.

6. Confidentiality and Information Security Standards

6.1. Processing will be subject to a strict duty of confidentiality: The Processor shall keep Personal Data strictly confidential and may only disclose Personal Data to third parties with the prior written consent of the Controller or as otherwise agreed in this Addendum. The Processor shall ensure that its employees are aware of the applicable privacy and information security requirements and are held by legally binding confidentiality obligations, which must survive the termination of their employment.

6.2. The Processor will ensure appropriate protection of Personal Data in accordance with the requirements of the Data Protection Rules and must implement appropriate operational, technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or Information Security Incidents and in light of the relevant risks presented by the Processing. In particular, this should include, but is not limited to:

6.2.1. Preventing access by unauthorized persons to Processing facilities and systems, where Personal Data is Processed or used (physical access control);

6.2.2. Preventing unauthorized use of Processing systems (admission control);

6.2.3. Ensuring that those persons authorized to use a Processing system are only able to access Personal Data within the scope of their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization during Processing, use and after recording (virtual access control);

6.2.4. Ensuring that, during electronic transfer, transportation or when being saved to data carriers, Personal Data cannot be read, copied, modified or deleted without authorization, and that it is possible to check and identify the points at which data transfer equipment is likely to be used to move Personal Data (transfer and disclosure control);

6.2.5. Ensuring that it will subsequently be possible to check and ascertain whether and by whom Personal Data has been accessed, modified or deleted from Processing systems (input control);

6.2.6. Ensuring that Personal Data Processed under the terms of this Addendum can only be Processed in accordance with the instructions issued by the Controller (assignment control);

6.2.7. Ensuring that Personal Data is protected against accidental malfunctions or loss (availability control); and

6.2.8. Ensuring that Personal Data collected for different purposes can be Processed separately (separation control).

6.3. The Processor represents and warrants that it has implemented the technical and organizational security measures described in Appendix 2.

6.4. The Processor will update the technical and organizational security measures in line with reasonable technological developments as determined by Processor. The Processor's technical and organizational measures and any material amendments thereto must be documented by the Processor and the Processor should provide this documentation to the

Controller on request (pursuant to Section 8.1 of this Addendum) in the form of its current ISO 27001 certification.

7. Cooperation and Notification Obligations

7.1. The Parties will co-operate with each other to promptly and effectively handle enquiries, complaints, and claims relating to the Processing of Personal Data from any government official or authority (including but not limited to any data protection or law enforcement agency), third parties or individuals (including but not limited to the Data Subjects). If a Data Subject should apply directly to the Processor to exercise his/her Personal Data rights, the Processor must forward this request to the Controller without delay, unless otherwise agreed between the Parties.

7.2. The Processor will notify the Controller of an Information Security Incident that is determined to affect Controller's Personal Data without undue delay. This notification must include the details of Personal Data compromised, including, but not limited to: (i) the nature of the Information Security Incident; (ii) the identity and contact details of a contact person; and (iii) the measures taken or proposed to minimize possible harm. The Processor will fully cooperate with and provide any additional information requested by the Controller to investigate the Information Security Incident.

7.3. The Parties are aware that the applicable Data Protection Rules may impose a duty to inform the competent authorities or affected Data Subjects in the event of the loss or unlawful disclosure of Personal Data or access to it. These incidents should therefore be notified by the Processor to the Controller without undue delay.

8. Controller's Audit and Inspection Rights

8.1. The Processor must ensure that the Controller can confirm the Processor's obligations under this Addendum and adherence to the information security measures and confidentially requirements under Sections 6 of this Addendum. For this purpose, the Processor must provide the Controller, upon request, with evidence of the implementation of these requirements which shall be evidenced by a current ISO 27001 certificate.

8.2. The Controller may inspect or audit the Processing work flows in the Processor's company at regular intervals in order to verify compliance by the Processor with the terms and conditions of this Addendum and in particular with the obligations relating to measures mentioned in Section 6.

8.3. The inspection may be carried out by the Controller's data protection officer or a representative of the Controller. No competitor of the Processor may be appointed as an auditor. The Controller will inform the Processor prior to any inspection. The Controller undertakes to carry out any inspection during normal working hours and without interfering with the course of the Processor's business.

8.4. The Controller and the Processor may be subject to control by public authorities. The Processor will notify the Controller immediately if the Personal Data is subject to a control or investigation by public authorities and will not disclose any Personal Data without the prior consent of the Controller. The Processor will provide the public authorities, upon request, with information regarding Processing under this Addendum as well as allow

inspections within the scope stated in this Section 8. The Processor will work together with the Controller, as specified in Section 7.1.

9. Use of Subcontractors

9.1. The Processor is entitled to subcontract with a third-party hosting facility. Any subcontractor must comply with applicable Data Protection Rules and be contractually bound by the same obligations arising from this Addendum, including but not limited to the information security measures and confidentiality provisions in Section 6, the cooperation and notification obligations in Section 7 and the audit and inspection rights in Section 8. For the avoidance of doubt, the Controller will be granted the same rights granted in these Sections (cooperation, notification, audit and inspection) vis-à-vis the subcontractor. The Processor will keep the Controller updated of any changes to the subcontracted Processing and provide the Controller with a copy of this subcontracting agreement upon request.

10. Return and Deletion of Personal Data

10.1. Upon the request of the Controller or upon termination of this Addendum, the Processor will, at the discretion of the Controller, return all Personal Data and the copies thereof to the Controller or will destroy all Personal Data and copies thereof and certify to the Controller that this has been done. Any disposal of Personal Data Processing media must comply with Data Protection Rules. Storage of Personal Data by the Processor is only allowed to the extent required by binding legislation, in which event the Processor must inform the Controller in writing of such requirements.

10.2. Upon termination of this Addendum, the Processor must not disclose any Personal Data without the prior consent of the Controller. Any retention of title claim of the Processor with respect to the aforementioned matters is expressly excluded. The Processor and its employees' obligations of confidentiality (provided in Section 6.1 of this Addendum) will remain in force.

11. Indemnification

11.1. Subject to Section 7 of the General Terms and Conditions, entitled "Limitation of Liability," provided that mandatory Data Protection Rules do not take precedence and unless stipulated otherwise in this Addendum or the Agreement, the Processor will fully reimburse the Controller, its Affiliates, subsidiaries and their respective officers, employees, and agents for:

11.1.1. All costs, liabilities, losses or expenses incurred by the Controller (including but not limited to fees, fines, penalties and third-party damages or claims) that were caused by the Processor's breach of this Addendum; and

11.1.2. All costs, liabilities, losses or expenses incurred by the Controller (including but not limited to fees, fines, penalties and third-party damages or claims) to:

a) remedy violations by the Processor or its subcontractor of the Data Protection Rules, information security laws, tort laws or other laws or regulations that directly or indirectly regulate the Processing;

b) defend all claims brought by as a result of the Processor's breach of this Addendum; or

c) satisfy a legal requirement caused by the Processor's or its subcontractors' breach of this Addendum.

11.2 The Controller shall indemnify Processor against all claims by any third party with regard to the processing of personal data provided to the Processor if the processing of such data was not permitted by data protection laws.

12. Miscellaneous

12.1. This Addendum together with its Appendices and the Agreement provide the principal terms for the relationship between the Parties.

12.2. The Parties also agree that no failure or delay in exercising any right, power or privilege under this Addendum will operate as a waiver thereof, nor will any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right under this Addendum

12.3. Amendments to this Addendum will be made in writing.

12.4. Should a provision of this Addendum be or become invalid, the validity of the other provisions of this Addendum will remain unaffected hereby. The Parties agree that, in the place of the invalid provision, a legally binding provision shall apply which comes closest to what the Parties would have agreed if they had taken the partial invalidity into consideration.

12.5. This Addendum will be construed and enforced in accordance with the laws of Minnesota. Each party irrevocably agrees to submit to the non-exclusive jurisdiction of the courts of Minnesota over any claim or matter arising under or in connection with this Addendum or the legal relationship established by this Addendum.

Controller	Processor
By:_____	By: _____
Name/Title: _____	Name/Title: _____
Date: _____	Date:_____

Appendix 1: Processed Personal Data and Purposes

The following Personal Data are transferred and Processed for the **following purpose**s:

Information related to the employees of Controller, and its subsidiaries will be uploaded into the Project for due diligence and sharing purposes by attorneys, tax professionals and other advisors.

Scope of Processing:

As described in the Statement of Work, Merrill will host documents in a virtual data room and provide access to the data room to attorneys, tax professionals, consultants and other advisors.

Categories of Personal Data:

The Personal Data concerns the following categories of data:

- Names and employers of employees
- Compensation and benefits information of employees
- Job titles and functions of employees

Special Categories of Data (if applicable):
The Personal Data concerns the following Special Categories of Data (please specify):

- N/A

Data Subjects:

The Personal Data concerns the following categories of Data Subjects:

- Employees

Processing operations:

The Personal Data will be subject to the following basic Processing activities (please specify):

- Upload and storage of personal data in a data room. No further processing operations contemplated.

Appendix 2: Information Security Measures

Appendix 2 is made up of:
Section I: Processor's General Data Security Plan
Section II: Processor's Information Security Procedure/Process

I. General Data Security Plan

	Security Requirement	How the Processor implements the specific information security measure
	Please describe the access control (physical) measures in your company to prevent unauthorized persons from gaining access to Processing systems within which Personal Data are Processed or used (If your company has several subsidiaries or branches please distinguish the differences between the locations).	All data centers hold ISO 27001:2013 and SOC 2 Type 2 certifications. In addition, the data centers are certified under the Privacy Shield Frameworks. A perimeter of multiple security controls are in place for all data centers which include multiple require authentication methods in order to gain access.
2.	Please describe the admission control measures taken in your company to prevent Processing systems from being used without authorization.	Authorized users are based on business requirements and require management role identification and approval. Time out features, strong authentication requirements and access rights are implemented and trackable.
3.	Please describe the access control (virtual) measures taken in your company to ensure that persons entitled to use a Processing system have access only to Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of Processing or use and after storage.	Authorized user access is managed through a formal registration and de-registration procedure for granting and revoking access to all systems and services based on job role. Audit reporting allows for the accurate monitoring of user activity and access controls are in place to protect data integrity and confidentiality.
4.	Describe the transmission control measures taken in your company to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.	Processor has removable media policy with the appropriate technical controls in place to protect data integrity and confidentiality and prohibit unauthorized Personal Data transfer. Remote access is controlled using multifactor authentication. Data is encrypted at rest and in-transit using government approved encryption technologies.

5.	Describe the measures of input control to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into Processing systems, modified or removed.	Processor is agnostic to the data the client chooses to upload. All user actions with respect to data integrity and confidentiality are tracked and reportable. Controller has sole determination on what data is provided to Processor.
6.	Describe the assignment control measures in your company to ensure that, in the case of commissioned Processing, the Personal Data are Processed strictly in accordance with the instructions.	Audits are conducted annually as part of ISO 27001 Certification and SOC 2 Type 2 Report to ensure compliance requirements are being met. Authorized users complete Training and acknowledge compliance with company code of conduct and policies annually. All employees and contractors are required to sign NDA.
7.	Describe the availability control measures your company takes to ensure that Personal Data are protected from accidental destruction or loss.	Processor has redundancy with each platform and maintains logs of system availability. In addition, redundancy allows for continuous system backups. Processor has Disaster Recovery and Business Continuity Plans that are reviewed, updated and tested annually.
8.	Describe the separation control measures your company has taken to ensure that Personal Data collected for different purposes can be Processed separately.	Logical separation is maintained within the same multi-tenant database. Authorized users are restricted to the project to which they are authenticated. Processor maintains a 3-tiered application with separation of data; development, test and production

II. Processor's Information Security Procedure/Process

The Processor implements and follows the following standards, processes, and procedures:
Merrill operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope: The management of information security applies to processes for the protection of client information regarding the global services of financial transactions and reporting, marketing and communications for regulatory industries, and customer content and collaborations.