ACCEPTANCE AND ACKNOWLEDGMENT OF TERMS

This Acceptance and Acknowledgment of Terms ("Agreement") confirms the agreement between You and the New York City Human Resources Administration ("Human Resources Administration") and the Mayor's Office of Public Engagement ("PEU") and the Mayor's Office of Strategic Policy Initiatives ("DemocracyNYC") (collectively, the "City") regarding Your participation in the Text Out the Vote ("TOTV") campaign. In order to participate in the TOTV campaign, You will require access to the Hustle peer-to-peer texting platform that the City has procured for these purposes (the "Product"). This Agreement shall govern Your use of the Product.

1. I am submitting my acceptance to this Agreement to the City, with the understanding that it will be relied upon by the City in connection with my participation in the TOTV campaign and that my participation is subject to acceptance of the terms below.

2. The City hereby grants Me a non-exclusive, royalty-free sublicense to use the Product in connection with the authorized uses, which shall consist of uses made by Me for purposes of participating in the TOTV campaign at the direction of the City and shall be in addition to and in compliance with the applicable terms for the Product. My use of the Product shall at all times be in accordance with the terms for the Product (the "License Terms") provided by Hustle, Inc. (the "Manufacturer"), including any privacy policy or terms of use embedded within or attached to the License Terms ("Supplemental Terms"), which are attached to the bottom of this Agreement as Attachment A. I am responsible for reading and acting in accordance with the License Terms and Supplemental Terms in Attachment A.

3. The license to the Products (the "Licenses") shall remain the sole property of the City. I shall make no use of the Product except as expressly provided herein, or as otherwise granted in advance in writing by the City or Mayor's PEU.

4. I shall not, except as this Agreement or the License Terms may expressly permit: (a) copy, modify, or create derivative works or improvements of the Product; (b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available the Product to any person; (c) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Product; (d) transmit any content, data or information that is unlawful, abusive, malicious, harassing, or violates any law or any privacy provisions contained within the License Terms; or (e) access the Product for the purpose of building a competitive product or service or copying its features or user interface.

5. I acknowledge that the City may suspend My use of the Product if, in the City's sole judgment (i) I have violated, am violating, or intend to violate any of the provisions contained in the License Terms; (ii) I am using the Product for fraudulent, misleading, or unlawful activities; (iii) My use of the Product disrupts or poses a security risk to the Product or to the information technology systems of the City or the Manufacturer, their clients or vendors, including introducing virus, worm, malware, or other malicious computer code through use of the Product.

6. I acknowledge my responsibilities under the License Terms as they are applicable to My use of the Product, and agree to comply with those provisions. I agree to provide all cooperation and assistance as the City or the Manufacturer may reasonably request to enable the City or the Manufacturer to exercise its rights and perform its obligations under the License Terms and in connection with the Product.

7. If I become aware of any actual or threatened activity prohibited by these Terms or the License Terms, I shall, without undue delay: (a) take all reasonable and lawful measures within My respective control that are necessary to stop the activity or threatened activity and to mitigate its effects (including, where applicable, by discontinuing and preventing any unauthorized access to the Product); and (b) notify the City of any such actual or threatened activity.8. I shall: (a) retain control over and responsibility for all information, instructions, and materials provided by or on behalf of the City in connection with the Product; and (b) safely administer the use of all identification numbers, passwords, licenses or security keys, security tokens, PINs, or other security codes, methods, technologies, or devices used, alone or in combination, to verify an individual's identity and authorization to access and use the Product and protect against any unauthorized access to or use of the Product.

9. Upon the expiration of my participation in the TOTV campaign or sooner termination by the City, I shall not have any right to use the Product and shall cease using the Product immediately.

10. To the fullest extent permitted by Law, I agree to defend, indemnify, and hold harmless the City, including its officials and employees, against any and all claims (even if the allegations of the claim are without merit), judgments for damages on account of any injuries or death to any person or damage to any property, and costs and expenses to which the City or its officials or employees, may be subject to or which they may suffer or incur allegedly arising out of My participation in the TOTV campaign and use of the Product under this Agreement to the extent resulting from any negligent act of commission or omission, any intentional tortious act, and/or the failure to comply with law or any of the requirements of this Agreement, or any alleged intellectual property infringement. Insofar as the facts or law relating to any of the foregoing would preclude the City or its officials or employees from being completely indemnified, the City and its officials and employees shall be partially indemnified to the fullest extent permitted by Law.

11. I agree to hold all Confidential Information obtained in connection with my participation in the TOTV campaign and/or my use of the Product as strictly confidential, in accordance with all applicable laws and regulations. Other than as provided for under this Agreement, I shall not disclose Confidential Information to any third parties nor make use of such Confidential Information for the benefit of another, nor publish, distribute, sell, or otherwise reveal Confidential Information without the prior written authorization of Mayor's PEU. For purposes of this Agreement, Confidential Information shall mean any and all information provided to or obtained or used by Me in connection with this Agreement, including but not limited to identifying information as defined in the New York City Administrative Code § 23-1201 and the Citywide Privacy Protection Policies and Protocols issued by the Chief Privacy Officer of New York City, as they may from time to time be modified. I shall notify the City immediately if I lose Confidential Information or if I know or suspect that someone has used or accessed Confidential Information without authorization. I shall cooperate with the City to investigate, mitigate, or prevent any further unauthorized uses of or access to Confidential Information. I shall not retain Confidential Information after my participation in the TOTV campaign, and I shall immediately destroy Confidential Information under my control when so requested by the City. The confidentiality provisions herein shall survive the expiration or termination of my participation in the TOTV campaign.

12. I acknowledge and agree that this Agreement will be governed and construed under the laws of New York, without regard to application of its conflict of laws principles.

13. I have been given a full opportunity to review and analyze this Agreement. I fully and completely understand all of the terms of this Agreement and sign it voluntarily, freely, and knowingly. The provisions of this Agreement shall become effective on the date of the signature set forth below.

AGREED AND ACCEPTED:

_____

SIGNATURE

_____

NAME

_____

DATE

ATTACHMENT A

1. SAAS SERVICES AND SUPPORT

1.1 Subject to these terms and conditions of use, in addition to any terms contained on an Order Form referencing these terms and the Cloud Services Rider attached hereto(collectively, the "Agreement") Hustle will provide Customer access to the Hustle software-as-a-service communication platform and related services as described in an applicable Order Form ("Services").

1.2 Subject to the terms hereof, Hustle will provide Customer with technical and customer support services in accordance with Hustle's standard practices then in effect and as described in an applicable Order Form, which is referenced and incorporated herein.

2. RESTRICTIONS AND RESPONSIBILITIES

2.1 Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, or algorithms relevant to the Services or any software, documentation or data related to the Services; modify, translate, or create derivative works based on the Services or any portion thereof(except to the extent expressly permitted by Hustle or authorized within the Services); use the Services for timesharing or service bureau purposes or otherwise for the benefit of a third party; or remove any proprietary rights notices.

2.2 The Services may be subject to export laws and regulations of the United States and other jurisdictions. Hustle and Customer each represents that it is not named on any U.S government denied-party list. Customer will not permit any user to access or use any part of the Service in a U.S.-embargoed country or region (currently Cuba, Iran, North Korea, Sudan, Syria or Crimea) or in violation of any U.S. export law or regulation.
2.3 Customer represents, covenants, and warrants that Customer will use the Services only in compliance with Hustle's Acceptable Use Policy located at hustle.life/aup, which is attached hereto as Exhibit A, (collectively the "Policy") as modified by the terms of this Agreement, and all applicable laws and regulations. Hustle reserves the right to determine whether to modify or amend the Policy and shall promptly provide notice of such amendment to Customer via email. Customer hereby agrees to indemnify and hold Hustle harmless against any damages, losses, liabilities, settlements and expenses (including without limitation costs and attorneys' fees) in connection with any claim or action that arises from an alleged violation of the Policy. Although Hustle has no obligation to monitor Customer's use of the Services, Hustle may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

2.4 Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "Equipment"). Customer shall also be responsible for maintaining the security of the Equipment, Customer account, passwords (including but not limited to administrative and user passwords) and files, and for all uses of Customer account or the Equipment with or without Customer's knowledge or consent.

2.5 Hustle reserves the right to permanently deactivate groups of contacts organized within Customer's Hustle account ("Hustle Groups") in which no messages have been sent for 89 or more days. Hustle also reserves the right to deactivate Hustle Groups Customer has selected to be archived.

3. CONFIDENTIALITY; PROPRIETARY RIGHTS

3.1 Each party (the "Receiving Party") understands that the other party (the "Disclosing Party") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "Proprietary Information" of the Disclosing Party). Proprietary Information of Hustle includes non-public information regarding features, functionality and performance of the Service. Proprietary Information of Customer includes non-public data provided by Customer to Hustle to enable the provision of the Services ("Customer Data"), including without limitation the names and phone numbers of volunteers. The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party or (e) is required to be disclosed by law.

3.2 Customer shall own all right, title and interest in and to the Customer Data. If Customer or any of its employees or contractors sends or transmits any communications or materials to Hustle by mail, email, telephone, or otherwise, suggesting or recommending changes to the Services, including without limitation, new features or functionality relating thereto, or any comments, questions, suggestions, or the like ("Feedback"), Customer retains all right, title and interest in and to the Feedback, and Hustle shall be free to use the Feedback. Hustle shall own and retain all right, title and interest in and to (a) the Services, all improvements, enhancements or modifications thereto (including, but not limited to, any improvements, enhancements or modifications to the Service based on Feedback), (b) any software, applications, inventions or other technology developed in connection with the Services or support, and (c) all intellectual property rights related to any of the foregoing.

3.3 Notwithstanding anything to the contrary, Hustle shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning Customer Data and data derived therefrom) in accordance with its privacy policy at https://www.hustle.com/privacy. ("Privacy Policy") attached hereto as Exhibit B, as modified by the terms of this Agreement. Hustle will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Hustle offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business. No rights or licenses are granted except as expressly set forth herein. In no case will such aggregate or de-identified data contain any Personal Identifying Information, as defined in Section 10-501(a) of the

Administrative Code of the City of New York, or Confidential Information as defined in Section 3 of this Agreement , nor shall it identify the City of New York specifically as the source of any such data.

4. PAYMENT OF FEES

4.1 Customer shall pay the third-party reseller that has sold, licensed, transferred or otherwise provided the Services to Customer ("Reseller") who shall pay Hustle the fees described in the Order Form for the Services as described in the Order Form in accordance with the terms therein. If Customer's use of the Services exceeds the Service capacity, if any, set forth on the Order Form or otherwise requires the payment of additional fees (per the terms of this Agreement), Reseller shall be billed for such usage and Customer agrees to pay Reseller the additional fees in the manner provided herein. Absent uncured material breach by Hustle, fees are nonrefundable or subject to allocation. Hustle reserves the right to change the Fees or applicable charges and to institute new charges and Fees at the end of the Initial Service Term or thencurrent renewal term, upon thirty (30) days prior notice to Customer (which may be sent by email). If Customer believes that Hustle has billed Customer incorrectly, Customer must contact Hustle no later than 30 days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Hustle's customer support department.

5. TERM AND TERMINATION

5.1 Subject to earlier termination as provided below, this Agreement is for the Initial Service Term as specified in the Order Form, and shall not automatically renew.

5.2 In addition to any other remedies it may have, either party may terminate this Agreement upon thirty (30) days' notice (or without notice in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement and such breach remains uncured for thirty days following notice thereof. In no event will termination relieve Customer of its obligation to pay Reseller any fees payable to Hustle for the period prior to the effective date of termination. All sections of this Agreement which by their nature should survive termination will survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, limitations of liability, and dispute resolution and arbitration provisions.

5.3 Upon termination, Customer Data shall remain available for Customer to download for 30 days. Upon request, Hustle shall delete all production Customer Data. Hustle may retain a secure, encrypted copy of Customer Data for up to one year after termination pursuant to Hustle's standard archiving and back-up procedures and policies. Hustle is subject to duties of confidentiality regarding Customer Data under this Agreement at all times that it is in Hustle's possession, in addition to Hustle's obligations under its Privacy Policy.

6. WARRANTY AND DISCLAIMER

6.1 Hustle shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Services in a

professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Hustle or by third-party providers, or because of other causes beyond Hustle's reasonable control, but Hustle shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption. However, Hustle does not warrant that the Services will be uninterrupted or error free; nor does it make any warranty as to the results that may be obtained from use of the Services. Hustle shall have no liability whatsoever for unavailability or interruption of the Services or any portion thereof, including but not limited to message delivery or phone call connectivity, for reasons beyond Hustle's control such as telecommunications network disruption, handset availability, carrier filtering rules or other issues with telecommunications providers. The Services may use or contain third party software (collectively, the "**Third Party Software**"). Hustle warrants that the Services do not infringe the intellectual property rights of any third party; provided, however, that Customer's sole remedy for Hustle's breach of this warranty shall be indemnification by Hustle as set forth in Section 7 below. As to Customer's use of the Services, Hustle bares full responsibility for the performance of the Third Party Software and any impact to the Services as a result of the Third Party Software and warrants that it has full right and title necessary to use the Third Party Software. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED "AS IS" AND HUSTLE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. INDEMNITY

7.1 Subject to the limitation of liability set forth in Section 8 below, Hustle shall hold Customer harmless from liability to third parties resulting from infringement by the Service of any United States patent or any copyright or misappropriation of any trade secret, provided Hustle is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement; Hustle will not be responsible for any settlement it does not approve in writing. The foregoing obligations do not apply with respect to portions or components of the Service (i) not supplied by Hustle, (ii) made in whole or in part in accordance with Customer specifications, (iii) that are modified after delivery by Hustle, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where Customer's use of the Service is not strictly in accordance with this Agreement. If, due to a claim of infringement, the Services are held by a court of competent jurisdiction to be or are believed by Hustle to be infringing, Hustle may, at its option and expense (a) replace or modify the Service to be non-infringing provided that such modification or replacement contains substantially similar features and functionality, (b) obtain for Customer a license to continue using the Service, or (c) if neither of the foregoing is commercially practicable, terminate this Agreement and Customer's rights hereunder and provide Customer a prorated refund of any prepaid, unused fees for the Service.

8. LIMITATION OF LIABILITY

8.1 NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, NEITHER CUSTOMRER NOR HUSTLE AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND HUSTLE'S REASONABLE CONTROL; OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID BY CUSTOMER TO HUSTLE FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY ("LIABILITY CAP"), IN EACH CASE, WHETHER OR NOT HUSTLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8.2 The Liability Cap Section 8.2 will not apply to liability arising out of any of the following: **(i)** the indemnification obligations under this Agreement; **(ii)** breach of Section 3 (confidentiality) in this Agreement **(iii)** breach of Section II or Section III of the Cloud Services Rider, **(iv)** the infringement by Hustle, or any of its affiliates or subcontractors, of the intellectual property of the City; (v) the infringement by Customer, or any of its affiliates or subcontractors, of the intellectual property of Hustle, and **(vi)** to the extent prohibited by law. With regard to a party's total and aggregate liability for any and all claims arising under Sections 8.1(i) and (iii), the Liability Cap shall be increased to $600,000.00.

9. MISCELLANEOUS

9.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

9.2 This Agreement is not assignable, transferable or sublicensable by Customer except with Hustle's prior written consent. Hustle may transfer and assign any of its rights and obligations under this Agreement without consent.

9.3 This Agreement, including any attachments, is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein.

9.4 No agency, partnership, joint venture, or employment is created as a result of this Agreement and Customer does not have any authority of any kind to bind Hustle in any respect whatsoever.

9.5 The parties shall endeavor to resolve any dispute with respect to this Agreement in good faith within 30 days of a dispute being raised by one party with the other party.

9.6 All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

9.7 This Agreement shall be governed by the laws of the State of New York without regard to its conflict of laws provisions. Hustle hereby consents to jurisdiction of the courts located in New York City for purposes of this Agreement.

9.8 Force Majeure. No party shall be liable or responsible to the other Party, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement except for any obligations to make payments to the other party hereunder, when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control ("Force Majeure Event"). The party suffering a Force Majeure Event shall give notice within 3 days of the Force Majeure Event to the other party, stating the period of time the occurrence is expected to continue and shall use diligent efforts to end the failure or delay and ensure the effects of such Force Majeure Event are minimized.

9.9 Public Announcements and Case Studies. Neither party shall use the other party's trademarks, service marks, trade names, logos, domain names or other indicia of source, affiliation or sponsorship, in each case, without the prior written consent of the other party. Hustle may, subject to obtaining Customer's consent, include Customer's name and/or other indicia in its lists of Hustle's current or former customers of Hustle in promotional and marketing materials.

Cloud Rider

ADDITIONAL TERMS AND CONDITIONS FOR CLOUD SERVICES AGREEMENTS

The additional terms and conditions of this Cloud Rider ("**Rider**") supplement the Hustle Terms and Conditions of Use and any applicable order form entered thereunder (collectively, the "Agreement") by Hustle, Inc., as the Cloud Service provider ("**Provider**"), and the City of New York (including any agency, office or commission), as licensee ("**City**" or "**Licensee**"), and are applicable to any procurement of hosted services from Provider). As used in this Rider, "party" refers to the City or the Provider (i.e., does not include a Reseller, if any) individually, and "parties" means the City and the Provider, collectively.

The parties hereby agree as follows:

I DEFINITIONS

1. "**City**" means the City of New York.

2. "**City Data**" means information, databases, data compilations, reports, charts, graphs, diagrams, or other information created, generated or maintained by Provider or its subcontractors for the benefit of the City under this Agreement or made accessible by the City to Provider under this Agreement. City Data includes, but is not limited to: electronically stored information ("ESI") that is supplied to Provider or its subcontractors by or on behalf of the City, and any copies of such ESI.

3.

4. "**Cloud Services**" means the Hustle software-as-a-service communication platform and related services as described in an applicable order form.

5. "**Cloud Terms**" means the Agreement referenced above, and is deemed to include the terms and conditions of this Rider.

6. "**Provider**" means the entity entering into this Agreement with the Department.

7. "**Department**" means the City agency that has entered into this Agreement.

8. "**DOITT**" means the City Department of Information Technology and Telecommunications.

9. "**Rider**" means these Additional Terms and Conditions for Cloud Services Agreements.

II DATA MANAGEMENT AND SECURITY

1. Safeguards to Protect City Data. Provider shall implement and maintain appropriate physical, technical, administrative, and organizational safeguards in accordance with industry best practices and applicable law to protect the security, confidentiality, availability, and integrity of City Data, including, but not limited to, the safeguards described in this Rider.

2. Backup and Recovery of City Data. As a part of the Cloud Services provided under this Agreement, Provider is responsible for creating, maintaining, and testing backup copies of City Data. Provider is responsible for an orderly and timely recovery of the Cloud Services and City Data in the event that the Cloud Services are interrupted. Except as otherwise provided in this Agreement, Provider will use best efforts to meet the recovery time objective ("**RTO**") for Cloud Services in twelve (12) hours and the recovery point objective ("**RPO**") for City Data in six (6) hours. For the purpose of calculating the RTO, recovery time is equal to the elapsed period of time between the commencement of an interruption and the time at which the Cloud Service is fully restored and available for use by

the City. RPO means the period of time during which changes made to data will not be included in a replication or other backup copy. Provider shall replicate data to a disaster recovery site that meets the requirements in this Rider. Provider shall maintain no less than thirty (30) days of backups. Any backups of City Data will not be considered in calculating storage used by the Department.

3. Disaster Recovery Sites. Provider shall have a minimum of one disaster recovery site at a distance from the primary site that is sufficient to protect against all hazards and consistent with industry best practices for business continuity. City Data must be replicated from the primary data center to the disaster recovery site in a in a commercially reasonable timeframe, and the Cloud Service must be configured to fail over from the primary data center to the disaster recovery site within a commercially reasonable timeframe. The disaster recovery site must be capable of supporting the Cloud Service at full load. The Department and City will not incur any costs in relation to additional recovery site(s).

4. Disaster Recovery Plans. Provider shall implement, maintain, and test disaster recovery plans to minimize downtime resulting from all hazards, including system failure. Provider represents that these disaster recovery plans are documented, tested no less frequently than once every twelve (12) months, and updated as required. The City has a right to review Provider's disaster recovery plans, and Provider must, upon the Department's request, provide the Department with a copy of such plans.

5. Data Availability, Storage, and Retention. Provider shall comply with the following:

(a) Provider shall ensure that all City Data is available to the Department at all times during the term of the Cloud Services and for a period of ninety (90) days after the term ends, including during any suspension of Cloud Services.

(b) All City Data uploaded by the City and stored by Provider shall be available to the City to copy back to the City's storage without alteration or loss and at no additional charge.

(c) Provider may use, access, or perform analytical analyses on data derived from the City's usage of the Cloud Service, for the purposes of internal evaluation to enhance the Services and in accordance with the privacy policy attached to the Agreement as Exhibit B and the provisions of the Cloud Terms and this Rider; (provided, however, under no circumstance will the City's use of the Services result in the serving of targeted advertisements) or as required for the Provider to provide the Cloud Service.

In accordance with Section 3.3 of the Cloud Terms, any use of data generated or supplied by the City will be for internal purposes only and to the extent it is shared with third-parties, all data shall be aggregated and de-identified and shall not contain any Personal Identifying Information, as defined in Section 10-501(a) of the Administrative Code of the City of New York, or Confidential Information as defined in Section 3 of the Cloud Terms, nor shall it identify the City of New York as the source of any data.

(d) City Data shall not be altered, moved, or deleted without the Department's consent or as otherwise permitted under the Rider;

(e) If legal mandates for data retention apply specifically to City Data, Provider shall comply with all such mandates communicated to the Provider in writing; and

(f) Provider agrees that City Data will remain in the United States.

6. Access to City Data. Provider shall implement identity and access control policies

and procedures in accordance with applicable law and industry best practices

7. Occurrences Affecting City Data. Provider shall implement, maintain, test and update an incident response plan in accordance with applicable law and industry best practices. In the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise: **(i)** the security, confidentiality, availability, or integrity of City Data (including, without limitation, the unauthorized or illegal acquisition, access, or alteration of City Data by an unauthorized person); or **(ii)** the physical, technical, administrative, or organizational safeguards put in place by Provider that relate to the protection of the security, confidentiality, availability, or integrity of City Data (each of the incidents described in this introductory paragraph to Section II(8) is a "**Security Incident**"), Provider shall:

(a) notify the Department as soon as practicable, but in no event later than twenty-four (24) hours after discovery of the Security Event, informing the City of the nature of the Security Incident, the harmful effects of which Provider is aware, and all actions Provider has taken and plans to take. For purposes of this Section II(8) a Security Incident is deemed to be discovered pursuant to the provisions of Section VIII of Incident Response Plan;

(b) cooperate with the City in investigating the occurrence, including by making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable;

(c) immediately remedying the Security Incident at Provider's expense in accordance with Provider's Incident Response Plan;

(d) breach or compromise;

(e) in the case of Personal Identifying Information, as defined in Section 10-501(a) of the Administrative Code of the City of New York ("**PII**"), at the City's request and pursuant to the City's express instructions as to form, content, scope, recipients, and timing, notify the affected individuals as soon as practicable but no later than required to comply with applicable law;

(f) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required period for monitoring services, for no less than twelve (12) months following the date of notification to such individuals;

(g) be responsible for recovering and/or recreating lost City Data in the manner and on the schedule approved by the Department without charge to the Department;

(h) bear the responsibility and all related costs for any Security Incident to the extent that the City (or its employees, subcontractors or affiliates) is not at fault, including the cost of any associated remedial actions or mitigation steps, credit monitoring, notification, regulatory investigations, fines, penalties, enforcement actions and settlements;

(i) to the extent the Incident Response Plan dated March 1, 2019 and previously provided to the City is updated or replaced with a new version, Provider shall provide such plan to the City within 30 days after such update or replacement; and

(j) provide the Department with the "lessons learned" document generated pursuant to the Incident Response Plan.

8. Termination for Security Incident. In the event of a Security Incident that is caused by Provider's failure to comply with this Rider, the City may terminate the Cloud Service for

cause on no less than fifteen (15) days' prior written notice. To be valid, notice of termination must be given within ninety (90) days after notification of the Security Incident was given to the City. Within thirty (30) days after Provider's receipt of a valid termination notice under this paragraph, all fees the City has already paid for services that were to be provided after the date of the termination notice shall be refunded to the City. In no case will the City be entitled to a refund of fees paid for Services already rendered. This provision is in addition to any rights that the City may have to recover damages under this Rider, the Cloud Terms, or pursuant to applicable law.

9. Attempted Breaches. At the Department's request, Provider must notify the Department of the occurrence of any attempted breaches of the security, confidentiality, availability, or integrity of City Data within twenty-four (24) hours after discovery of the occurrence of an attempted breach.

10. Notice in Event of Provider Receipt of Warrant, Subpoena, or other Governmental Request. If Provider is served with a warrant, subpoena or any other order or request from a court or government body or any other person for any City Data, Provider shall, as soon as reasonably practical and not in violation of law, deliver a copy of such warrant, subpoena, order, or request to the Department.

III DATA PRIVACY AND INFORMATION SECURITY PROGRAM

1. Provider Privacy and Security Program. Without limiting Provider's obligation of confidentiality, as further described in this Agreement, Provider shall be responsible for establishing and maintaining a data privacy and information security program ("**Privacy and Security Program**") that includes reasonable and appropriate physical, technical, administrative, and organizational safeguards, to: **(A)** ensure the security, confidentiality, availability, and integrity of City Data; **(B)** protect against any anticipated threats or hazards to the security, confidentiality, availability, or integrity of City Data; **(C)** protect against unauthorized or illegal disclosure, access to, or use of City Data; **(D)** ensure the proper disposal of City Data, if requested by the City or required by applicable law; and, **(E)** ensure that all employees, agents, and subcontractors of Provider comply with all of the foregoing..

2. Security Controls. Provider's privacy and security controls must include, but not be limited to, physical, administrative, software, and network security measures, employee screening, employee training and supervision, and appropriate agreements with employees and subcontractors.

3. Audits

(a) Audit by Provider. No less than annually, Provider shall conduct a comprehensive audit of its Privacy and Security Program and provide such audit findings to the City.

(b) Right of Audit by City. Without limiting any other audit rights of the City, the City shall have the right to review and audit Provider's Privacy and Security Program prior to the commencement of this Agreement and no less than once annually during the term of this Agreement. The review and audit may be conducted remotely or onsite by the City or a City Provider and at the City's expense. The City shall conduct on-site audits in a manner so as not to unreasonably interfere with Provider's business operations. In lieu of an on-site audit, upon request by the City, Provider shall complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by the City regarding Provider's Privacy and Security Program. Provider shall not be entitled to compensation from the City for the time it

spends cooperating with any of the audits, scans, or tests provided for in this Section III(3), or in completing any audit questionnaire(s).

(c) Findings. Provider shall provide the City with a copy of all reports generated for each audit, scan, and test within ten (10) days after its completion. Each report must: **(A)** indicate whether any material vulnerabilities, weaknesses, gaps, deficiencies, or breaches were discovered; and **(B)** if so, describe the nature of each vulnerability, weakness, gap, deficiency, or breach. Provider shall, at its own cost and expense, promptly remediate each vulnerability, weakness, gap, deficiency, or breach that is identified in a report and provide the City with documentation of the remedial efforts within thirty (30) days after their completion.

(d) Performance Testing. Performance testing is required for all public-facing applications. Provider must demonstrate the ability to conduct performance testing and establish terms for testing and cost.

4. Vulnerabilities. Provider must provide vulnerability scanning services for critical systems or systems hosting sensitive data. Provider must provide attestation by an objective third party, stating that the application has been tested for known security vulnerabilities, including, without limitation, the "OWASP Top-10" as published by the Open Web Application Security Project (see www.owasp.org for current list of the top 10).

5. Change in Service. Provider shall notify the Department of any enhancement, upgrade, or other change in the Cloud Service that may impact the security, availability, or performance of the Cloud Services.

IV VENDOR INDUCED INHIBITING CODE AND HARDSTOP/PASSIVE LICENSE MONITORING

Provider shall not include any vendor induced inhibiting code ("**VIIC**") or any other inhibitor in the Cloud Services or on reports and data submitted and provided to the City under this Agreement. VIIC means any deliberately included application or system code that will degrade performance, result in inaccurate data, deny accessibility, or adversely affect, in any material way, programs or data or use of the Cloud Services.

V ENCRYPTION

1. Provider shall encrypt all City Data, including backups, while at rest and in transmission from end to end using encryption standards and methods that are approved and recommended by NIST.

2. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of Provider and approved in writing by the Citywide Chief Information Security Officer. Proven algorithms must be used as the basis for encryption technologies. At a minimum, the preferred hash algorithm is 160bit SHA-1. 128bit MD5 is an acceptable alternative. SSL/TLS implementations should use either 3-DES or AES for the cipher component and 128bit MD5 or 160bit SHA-1 for the digest cipher.

VI DOITT SECURITY REVIEW OF PROVIDER'S CLOUD SERVICES

1. This Agreement is subject to a security review by DOITT of Provider's Cloud Services. Such a security review has been completed.

2. Any written disposition of a security review by DOITT will not be deemed to constitute an endorsement of the Cloud Services or a certification that the Cloud Services meet the requirements under this Rider. Provider remains fully responsible for

ensuring compliance with this Rider. At all times during the term of the Cloud Services, Provider agrees to cooperate with DOITT to ensure that Provider is in compliance with all provisions of this Rider.

VII DATA OWNERSHIP

1. The City retains sole ownership and intellectual property rights in and to all City Data. Provider shall not use the City Data for any purpose other than as required to provide the Cloud Services to the Department or as otherwise permitted under the Agreement. Provider shall not retain any City Data after the ninety (90) day period identified in Section IX(1)(a), except as otherwise stated in the Agreement.

2. Except as expressly provided in this Rider or the Agreement, no ownership right or license to use, sell, exploit, copy or further develop City Data, any confidential information or intellectual property of the City is conveyed to Provider.

VIII NO SUPPLEMENTARY AGREEMENTS OR TERMS; NO UNILATERAL CHANGES:

1. All click-through, click-wrap, or shrink-wrap agreements or other end user terms and conditions that are embedded in or provided with any of Provider's Cloud Services or presented to users in the course of the Department's use of the Cloud Services that directly affect the contractual relationship between the Parties, the negotiated terms of the Rider and the Cloud Terms, or any rights or obligations as between the Parties are not applicable to the Department, even if use of Provider's Cloud Services require an affirmative acceptance of those terms. The terms and conditions of the Cloud Terms, including any exhibits, and this Rider are in static form, and no online terms and conditions that are incorporated by reference in the Cloud Terms or set forth in hyperlinked websites are binding on the City.Neither this Rider, nor the Cloud Terms, may be changed unilaterally. To be valid, any amendment to the Cloud Terms or this Rider must be in writing and signed by the parties.

IX SEPARATION ASSISTANCE

1. In the event of impending or actual separation (due to impending or actual expiration or earlier termination of this Agreement whenever that may occur) and for up to ninety (90) days following such expiration or termination, the Department may request in writing that Provider do or permit the City to do any of the following, or any combination of the following:

(a) Export and/or copy City Data, subject to any applicable charges as provided in this Agreement. If the Department requests an export of City Data, such exported data shall be in Newline Delimited JSON format.

(b) Destroy any City Data. Any written request by the Department directing Provider to destroy City Data shall specify what data the Department is requesting to be destroyed. Provider shall not destroy any City Data in the absence of a specific written request from the Department. If Provider destroys any City Data, it shall verify such destruction in writing.

2. Provider must provide separation assistance to the Department to perform or support the exporting, copying, and/or destruction of City Data in accordance with the Department's written request.

3. Transition Assistance will be provided at no cost to the City in the event of a termination by the City due to a breach by Provider of this Rider or the Cloud Terms.

X SUPPORT

1. Provider shall provide support to the Department in connection with the Cloud

Services in accordance with the applicable order form, which include (1) texting/in-application/web support during the hours of 9 a.m. to 5 p.m. PST Monday – Friday, excluding U.S. national holidays, and (2) online access to training guides and materials.

XI GENERAL

1. Order of Precedence. This Rider takes precedence over any provision in the Cloud Terms pertaining to City Data and the security thereof.

2. **Survival. All terms of this Rider that should by their nature survive termination will survive, including, Section II (Data Management and Security), Section III (Data Privacy and Information Security Program).**

3. Authorized User. The authorized user of the Cloud Service is the City of New York, including its employees, authorized agents, consultants, auditors, other independent Providers and any external users contemplated by the parties. This paragraph does not modify the quantity of users permitted to use the Cloud Service.

4. Insurance

(a) Data Breach and Privacy Cyber Liability & Errors and Omissions. Provider shall maintain at all times during the provision of Cloud Services, and as otherwise required herein, data breach and privacy cyber liability insurance with limits of no less than $10,000,000 per claim and $10,000,000 in the aggregate. This policy must include coverage for: **(A)** failure to protect confidential information, including personally identifiable information, **(B)** failure of the security of Provider's computer systems, **(C)** failure of the security of the City's systems or City Data due to the actions or omissions of the Contractor.

(1) This policy must include coverage for:

(A) Data breach expenses, including forensic services, the cost of complying with privacy laws and regulations, legal representation, notification costs, public relations and crisis management costs, credit monitoring, fraud consultation, credit freezing, fraud alert, and identity restoration services;
(B) Costs arising from cyber extortion threats, including the payment of ransom demands;
(C) The alteration, loss, corruption of data, including costs to recover, correct, reconstruct, and reload lost, stolen, or corrupted data;
(D) The cost of replacing, repairing, or restoring computer systems, including hardware (including laptops and mobile devices), software, networking equipment, and storage;
(E) Costs arising from an attack on a network or computer system, including denial of service attacks, malware, and virus infections;
(F) dishonest, fraudulent, malicious, or criminal use of a computer system by a person, whether identified or not, and whether acting alone or in collusion with other persons;
(G) media liability; and

(b) General Insurance Requirements

(1) All required insurance policies must be maintained with companies that may lawfully issue the policy and have an A.M. Best rating of at least A- / "VII" or a Standard and Poor's rating of at least A, unless prior written approval is obtained from the City Law Department.
(2) The City's limits of coverage for all types of insurance required under this Article shall be the greater of **(A)** the minimum limits required in this Rider, or **(B)** the limits provided to Provider as named insured under all primary, excess, and umbrella policies of that type of coverage.

(3) If Provider receives notice from an insurance company or other person that any insurance policy required under this Rider will expire or be cancelled or terminated for any reason, Provider shall immediately forward a copy of such notice to both the New York City Public Engagement Unit, [insert appropriate address], and the New York City Comptroller, Attn: Office of Contract Administration, Municipal Building, One Centre Street, Room 1005, New York, New York 10007.

(4) Insurance coverage in the minimum amounts required in this Article will not relieve Provider or its subcontractors of any liability, nor will it preclude the City from exercising any rights or taking such other actions as are available to it.

(5) Provider waives all rights against the City, including its officials and employees, for any damages or losses that are covered under any insurance required under this Rider (whether or not such insurance is actually procured or claims are paid thereunder) or any other insurance applicable to the operations of Provider or its subcontractors in the performance of Cloud Services.

(6) All claims-made policies must have an extended reporting period option or automatic coverage of not less than two (2) years. If available as an option, Provider shall purchase extended reporting period coverage effective on cancellation or termination of the claims-made insurance unless a new policy is secured with the same retroactive date as the expired policy.

EXHIBIT A

Acceptable Use Policy

The following shall apply to and govern your use of Hustle, Inc. ("Hustle")'s Services ("Services"). The Services may not be used in any manner that: (i) is illegal; (ii) is non-compliant with accepted industry best practice guidelines, (iii) disrupts or damages any of Hustle's computer systems or network or other parties' computer systems and networks, or (iv) violates any person's rights. If you do not agree to this Policy, do not use Hustle Services.

Hustle in its sole discretion shall determine whether there has been a violation of this Policy. Hustle may amend this Policy from time to time.

The following list of provides examples of prohibited uses. The list is provided by way of example and should not be considered exhaustive.

Prohibited uses include use of the Hustle Services to:

- Engage in any messaging in violation of any relevant laws or regulations (which may include and are not limited to, the Telephone Consumer Protection Act and the Do Not Call provisions of the Telemarketing Sales Rule)
- Engage in any messaging that is offensive, obscene, libelous, defamatory, fraudulent, abusive, or contains tortious material.
- Engage in messaging that is unsuitable for minors.
- Engage in messaging that promotes, incites or instructs on criminal matters.
- Engage in messaging that is false, misleading or deceptive, or likely to mislead or deceive.
- Engage in messaging that infringes the intellectual property rights or other rights of a third party.
- Engage in messaging that is otherwise unlawful.
- In addition, you will honor immediately any requests to opt-out or stop further messaging (e.g., any "STOP" messages), and desist from sending any further message following receipt of any such opt-out or stop request.

Violation of this Policy may result in termination or suspension of all services provided by Hustle and may also result in civil, criminal, or administrative liability or penalties against the client and those assisting the client.

Any failure to enforce this Policy does not amount to a waiver of Hustle's rights.

Contact Information

To ask questions or comment about these Subscriber Terms and our privacy practices, contact us at:

Hustle, Inc. 717 Market St., Floor 5 San Francisco, California 94103 or security@hustle.com.

EXHIBIT B

Privacy Policy

Hustle, Inc. (“Hustle,” “we,” “our,” or “us”) is committed to protecting your privacy. This Privacy Policy applies to our business customers (“Customers”) and Message Recipients (defined below) and explains how your personal information is collected, used, and disclosed by Hustle. This Privacy Policy applies to our website, Hustle.com, Hustle.life and our web and mobile apps (collectively, our “Service”). Hustle is a business to business service provider whereby Hustle provides notification and messaging services that allows our Customers to contact and send messages and information to their message recipients (“Message Recipients”) through mobile text messaging services. Customers generally use the Services via their agents and administrators, who are individuals designated by the Customer; a Customer’s agents send and receive the messages on behalf of the Customer, and a Customer’s administrators administer the Service on behalf of the Customer. Our Privacy Policy primarily explains our data collection practices when collecting, storing and or using data on behalf of our Customers as a service provider. If you are an individual Message Recipient who received a message from a Customer through Hustle and you wish to learn about how Hustle collects and uses your data, please see Section 1.2 below. If you wish to opt-out from receiving additional messages, please see Section 5 below.

By accessing or using our Service, you signify that you have read, understood, and agree to our collection, storage, use, and disclosure of your personal information as described in this Privacy Policy, our Terms & Conditions of Use, and your Order Form and associated agreement (as applicable). “You” or “your” means an authorized user on the Service associated with a Hustle Customer account and may include (without limitation), an employee, agent, volunteer, or administrator of Customer.

1. WHAT INFORMATION DO WE COLLECT AND FOR WHAT PURPOSE?

1.1 The categories of information we collect can include:

- **Information you provide to us directly.** We may collect personal information, such as your name, administrator/agent names, mobile phone numbers, location, payment information, email address, and other information about your company/organization when you register for our Service, sign up for our mailing list, or otherwise communicate with us. Customers also generally provide the full name, short name, phone number, and email address of their agents and administrators. We may also collect any communications between you and Hustle and any other information you provide to Hustle.
- **Information collected through your use of the Service.** We collect information about how you use the Service, your actions on the Service, and content you post to the Service, including information on Message Recipients (e.g., names, phone numbers and group designations) and their contact information, messaging scripts, photos and videos you post to the Service, and any other content you provide through other functionalities of the Service (“User Content”). Please remember that Hustle may, but has no obligation to, monitor, record, and store User Content in order to protect your safety or the safety of other users, to assist with regulatory or law enforcement efforts, or to protect and defend our rights and property. By using the Service, you consent to the recording, storage, and disclosure of such communications you send or receive for these purposes.

- **Text message content and related metadata.** We collect certain data about your messages and the content of your messages with Message Recipients, such as the content of messages you send and receive, message timestamps, message length, reply rates other statistics and metadata ("Text Message Data"). We use this Text Message Data for our internal purposes such as data analysis, fraud prevention, developing and improving our Service, and identifying usage trends. For example, we may build recommendations into our Services based on aggregated and anonymized Text Message Data. Note that any messages you send that are transmitted via Hustle may be accessible by certain third-party organizations, such as cellular networks and SMS gateway services, that may be used to transmit the messages. These organizations may have their own rules, policies, and security measures controlling who has access to messages transmitted through their services.
- **Information we receive from third parties.** From time to time, we may receive information about you or Message Recipients from third parties and other users. We may also collect information about you that is publicly available, or if you share information with us via a social network (such as "liking" us on a social media site), in accordance with the terms of those sites.

We use this information to operate, maintain, and provide to you the features and functionality of the Service, as well as to communicate directly with you, such as to send you email messages and push notifications, or invite others to join the Service. We may also send you Service-related emails or messages (e.g., account verification, updates to features of the Service, technical and security notices). We may also use this information for our internal business purposes, such as data analysis, audits, fraud prevention, developing new products, services, and/or features, improving our Service, identifying usage trends, and determining the effectiveness of our Service. For more information about your communication preferences, see "Control Over Your Information" below.

1.2 **CCPA Disclosures.** The California Consumer Privacy Act of 2018 ("CCPA"), expected to take effect on January 1, 2020, is anticipated to require certain companies to make disclosures about which Personal Information, as defined in the current version of the CCPA ("Personal Information") is collected, and shared or sold with third parties. In the spirit of a forward-thinking approach towards compliance with CCPA's privacy policy disclosure requirements, this section sets forward the categories of Personal Information collected, shared, and sold by Hustle.

- **Categories of Personal Information Collected:** Customers provide information, including Personal Information of Message Recipients, to Hustle via their customer relationship management ("CRM") integration with the Hustle Platform, by uploading the information in a CSV file, or by entering it directly in the Hustle Platform.
- **What Hustle Collects at a Minimum:** Message Recipient Personal Information provided to Hustle varies by the Customer and depends on what they transfer from their CRM/CSV file to the Hustle Platform, but this information at a minimum always includes the Message Recipient's first name, last name, and telephone number. In addition, Hustle obtains the IP Address of the Customer's admin & agent users, as well as the agent's unique phone device IDs. Customers also generally provide the full name, short name, phone number, and email address of their agents and administrators. This information is collected by Hustle solely to provide its Services to Customers and to improve and enhance its Service.
- **Other Information Hustle Might Collect.** In addition to the above, Customers may provide Hustle with additional Message Recipient Personal Information by manually entering it into a "custom field" or creating a "tag" within the Hustle Platform. Again, this depends on what a particular Customer decides to provide but may include (a) postal address; (b) limited education information in certain circumstances

(limited to school attended or field of study); (c) characteristics of protected classifications under California or federal law; and (d) professional or employment-related information. Hustle may use this information to draw inferences from the categories identified in this section to create a profile about a Message Recipient reflecting the Message Recipient's preferences, characteristics, psychological trends, preferences, predispositions, behavior, or attitudes. Hustle may also may collect browsing behavior and device and browser metadata, as well as metadata about voice calls.

- **Personal Information Shared:** In the course of using the Services, Customers are able to sync, and control the movement of, Personal Information between the Customer-operated platforms on which Personal Information resides (e.g., CRM platforms and other third-party services and platforms) ("Customer-Operated Platforms") and the Hustle Platform. As a result of this back-and-forth movement of Personal Information at the Customer's behest, Hustle by definition shares this Personal Information with the Customer-Operated Platforms and therefore with the entities that own and control these platforms. For example, a Customer may take Personal Information residing within a CRM platform (such as a Message Recipient's name and phone number) and share it with the Hustle Platform so it may contact that Message Recipient via the Hustle Platform. Later, that same Customer may take that Message Recipient's Personal Information, along with relevant information pertaining the Customer's interaction with the Message Recipient via the Services (such as whether the Message Recipient opted-out, interacted, etc.) and sync that Personal Information back into the CRM platform. By enabling Customers to perform these activities and other similar integrations, Hustle must share the Personal Information with the Customer-Operated Platforms. This is the business purpose for Hustle sharing Personal Information.
- **Personal Information Sold to Third Parties:** Hustle does not sell any Personal Information to any third party.

2. HOW WE USE COOKIES AND OTHER TRACKING CONTENT

We, and our third-party partners, automatically collect certain types of usage information when you visit our Service, read our emails, or otherwise engage with us. We typically collect this information through a variety of tracking technologies, including cookies, web beacons, embedded scripts, location-identifying technologies, file information, and similar technology (collectively, "tracking technologies"). For example, we collect information about your device and its software, such as your IP address, browser type, Internet service provider, platform type, device type, operating system, date and time stamp (a unique ID that allows us to uniquely identify your browser, mobile device, or your account), and other such information. We also collect information about the way you use our Service, for example, the site from which you came and the site to which you are going when you leave our website, the pages you visit, the links you click, how frequently you access the Service, whether you open emails or click the links contained in emails, whether you access the Service from multiple devices, and other actions you take on the Service. When you access our Service from a mobile device, we may collect unique identification numbers associated with your device or our mobile application (including, for example, a UDID, Unique ID for Advertisers ("IDFA"), Google AdID, or Windows Advertising ID), mobile carrier, device type, model and manufacturer, mobile device operating system brand and model, phone number, and, depending on your mobile device settings, your geographical location data, including GPS coordinates (e.g., latitude and/or longitude) or similar information regarding the location of your mobile device, or we may be able to approximate a device's location by analyzing other information, like an IP address. We may collect analytics data or use third-party analytics tools such as Google Analytics to help us measure traffic and usage trends for the Service and to understand more about the demographics of our users. You can learn more about Google's practices

at http://www.google.com/policies/privacy/partners and view its currently available opt-out options at https://tools.google.com/dlpage/gaoptout. We may also work with third-party partners to employ technologies, including the application of statistical modeling tools, which permit us to recognize and contact you across multiple devices. Although we do our best to honor the privacy preferences of our users, we are unable to respond to Do Not Track signals set by your browser at this time.

We use or may use the data collected through tracking technologies to: (a) remember information so that you will not have to re-enter it during your visit or the next time you visit the site; (b) provide custom, personalized content and information, including targeted content and advertising; (c) recognize and contact you across multiple devices; (d) provide and monitor the effectiveness of our Service; (e) monitor aggregate metrics such as total number of visitors, traffic, usage, and demographic patterns on our Service; (f) diagnose or fix technology problems; and (g) otherwise to plan for and enhance our Service.

If you would prefer not to accept cookies, most browsers will allow you to: (i) change your browser settings to notify you when you receive a cookie, which lets you choose whether or not to accept it; (ii) disable existing cookies; or (iii) set your browser to automatically reject cookies. Please note that doing so may negatively impact your experience using the Service, as some features and services on our Service may not work properly. Depending on your mobile device and operating system, you may not be able to delete or block all cookies. You may also set your email options to prevent the automatic downloading of images that may contain technologies that would allow us to know whether you have accessed our email and performed certain functions with it.

We and our third-party partners may also use cookies and tracking technologies for advertising purposes. For more information about tracking technologies, please see “Third Party Tracking and Online Advertising” below.

3. SHARING OF YOUR INFORMATION

We may share your personal information in the instances described below. For further information on your choices regarding your information, see the “Control Over Your Information” section below.

We may share your personal information with:

- Other companies and brands owned or controlled by Hustle, and other companies owned by or under common ownership as Hustle, which also includes our subsidiaries (i.e., any organization we own or control) or our ultimate holding company (i.e., any organization that owns or controls us) and any subsidiaries it owns. These companies will use your personal information in the same way as we can under this Privacy Policy;
- Third-party vendors and other service providers that perform services on our behalf, as needed to carry out their work for us, which may include identifying and serving targeted advertisements, providing mailing services, providing tax and accounting services, web hosting, or providing analytics services;
- The public when you provide feedback on our Service. For example, if you post user content on our blog or comment on our social media sites, your information, such as your first name, last initial, state of residence, and your comments, may be displayed on our Service or on our social media pages;

- Other parties in connection with a company transaction, such as a merger, sale of company assets or shares, reorganization, financing, change of control or acquisition of all or a portion of our business by another company or third party, or in the event of a bankruptcy or related or similar proceedings. In such event, Hustle will endeavor to direct the acquirer to use and protect and use your personal information in a manner that is consistent with the privacy policy in effect at the time such personal information was collected; and
- Third parties as required by law or subpoena or if we reasonably believe that such action is necessary to (a) comply with the law and the reasonable requests of law enforcement; (b) to enforce our Terms & Conditions of Use or to protect the security or integrity of our Service; and/or (c) to exercise or protect the rights, property, or personal safety of Hustle, our visitors, or others. This is subject to the terms of our Customer Notification Policy set forth in Section 8 below.

We may also share information, including User Content and Text Message Data, with third parties and other Hustle Customers in an aggregated or otherwise anonymized form, such as aggregated user statistics, that does not reasonably identify you or your Message Recipients directly as individuals. Please see the "Control Over Your Information" section for more information.

4. CONTROL OVER YOUR INFORMATION

How to control your communications preferences. You can stop receiving promotional email communications from us by clicking on the "unsubscribe link" provided in such communications. In addition, if a Customer receives a promotional text from Hustle, that Customer may opt-out of future promotional texts by texting "STOP" in response. We make every effort to promptly process all unsubscribe requests. You may not opt out of service-related communications (e.g., account verification, transactional communications, changes/updates to features of the Service, technical and security notices). Customer's agents and administrators who no longer wish to perform the agent or administrator functions can contact the particular Hustle Customer and request removal from groups.

Deleting Customer information. Unless otherwise agreed in writing, upon Customer's request, Hustle will delete all Hustle Customer production data, including personally identifiable information uploaded to the Service by that Hustle Customer. We may not be able to delete your information in all circumstances. For example, we may retain and use your information as necessary to comply with our legal obligations, resolve disputes, or enforce our agreements. Hustle may also retain a secure, encrypted copy of Customer Data for up to one year after termination pursuant to Hustle's standard archiving and back-up procedures and policies.

5. MESSAGE RECIPIENT OPT-OUT OF CUSTOMER MESSAGES THROUGH HUSTLE

We offer services enabling our Customers to send text messages through our Service. This Section discusses how individuals who receive a message from a Hustle Customer may opt-out of receiving messages from any particular Hustle Customer Campaign. To unsubscribe from any Hustle Customer texting campaign, Message Recipient recipients may text "STOP," "UNSUBSCRIBE" or similar words or phrases as a response to the sender or contact us via email at support@hustle.life. Hustle will send the Message Recipient one follow-up text message to confirm that the Message Recipient has been unsubscribed. In the event the Message

Recipient uses the Service with multiple Hustle Customers, we may send the Message Recipient a follow-up message to clarify which Customer from whom the Message Recipient would like to stop receiving messages. Message Recipients may also email us at support@hustle.life in the event they believe that a Hustle Customer has added their information in error or without their permission. Please note that opt-outs are tracked separately for each Hustle Customer, so unsubscribing from one Hustle Customer will not unsubscribe you from communications from another Hustle Customer.

To restart receiving text messages from a Hustle Customer, Message Recipients may text START to the Customer's short code or long code. In the event Message Recipients use the Service with multiple Hustle Customers, we may send an automated message to clarify which customer the Message Recipient wants to restart receiving messages and calls from. Standard message and data rates apply.

6. THIRD-PARTY TRACKING AND ONLINE ADVERTISING

If you visit our website, you should note that we participate in interest-based advertising and use third party advertising companies to serve you targeted advertisements based on your online browsing history and your interests. We permit third party online advertising networks, social media companies and other third party services, to collect, information about your use of our Sites over time so that they may play or display ads on our Sites, on other websites, apps or services you may use, and on other devices you may use. Typically, though not always, the information used for interest-based advertising is collected through cookies or similar tracking technologies. We may share a common account identifier (such as an email address or user ID) or hashed data with our third party advertising partners to help identify you across devices. We and our third party partners use this information to make the advertisements you see online more relevant to your interests, as well as to provide advertising-related services such as reporting, attribution, analytics and market research.

To learn more about interest-based advertising and how you may be able to opt-out of some of this advertising, you may wish to visit the Network Advertising Initiative's online resources, at http://www.networkadvertising.org/choices, and/or the DAA's resources at http://www.aboutads.info/choices. You may also be able to set your browser to delete or notify you of cookies by actively managing the settings on your browser or mobile device. Please note that some advertising opt-outs may not be effective unless your browser is set to accept cookies. Furthermore, if you use a different device, change browsers or delete the opt-out cookies, you may need to perform the opt-out task again.

You may also be able to limit certain interest-based mobile advertising through the settings on your mobile device by selecting "limit ad tracking" (iOS) or "opt-out of interest based ads" (Android).

Google Analytics and Advertising. We may also utilize certain forms of display advertising and other advanced features through Google Analytics, such as Remarketing with Google Analytics, Google Display Network Impression Reporting, and Google Analytics Demographics and Interest Reporting. These features enable us to use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick advertising cookie) or other third-party cookies together to inform, optimize, and display ads

based on your past visits to the Sites. You may control your advertising preferences or opt-out of certain Google advertising products by visiting the Google Ads Preferences Manager, currently available at https://google.com/ads/preferences, or by vising NAI's online resources at http://www.networkadvertising.org/choices.

7. HOW WE STORE AND PROTECT YOUR INFORMATION

Data storage and transfer: Your information collected through our Service may be stored and processed in the United States or any other country in which Hustle or its parent, subsidiaries, affiliates, or service providers maintain facilities. If you are located in other regions with laws governing data collection and use that may differ from U.S. law, please note that we may transfer information, including personal information, to a country and jurisdiction that does not have the same data protection laws as your jurisdiction.

Data retention: We will retain your personal information only for as long as reasonably necessary to maintain the Service, to meet legal and accounting obligations, and for the purposes described in this Privacy Policy. We may anonymize and/or aggregate personal information, including User Content and Text Message Data, and store it in order to analyze aggregate metrics and trends.

Keeping your information safe: We care about the security of your information and employ physical, administrative, and technological safeguards designed to preserve the integrity and security of all information collected through our Service. However, no security system is impenetrable, and we cannot guarantee the security of our systems 100%. In the event that any information under our control is compromised as a result of a breach of security, we will take reasonable steps to investigate the situation and, where appropriate, notify those individuals whose information may have been compromised and take other steps, in accordance with any applicable laws and regulations.

8. CUSTOMER NOTIFICATION POLICY

Civil Legal Processes: Hustle's policy is to notify Customers upon receipt of a civil subpoena demand of their account information or any associated data stored with Hustle. A two week wait period must transpire before disclosure of any information. Hustle will advise the Customer that the information will be disclosed unless Hustle is in receipt of a document seeking a court-approved protective order prior to the date on which Hustle must legally comply with the demand. Hustle will notify Customers upon receipt of legal process.

Fees for Civil Subpoena Processing: Hustle charges a fee for the processing of civil subpoenas, as authorized under 18 U.S.C. § 2706. This fee is set at $200/hour, with a two hour minimum per response. In addition, a per-subpoena fee of $50 per Customer whose data is requested shall be charged. No charge shall be required relating to matters involving the distribution of child pornography or any act of child endangerment. Furthermore, no charge shall be required to investigate matters dealing with abuse of Hustle's services to harass, abuse or intimidate any person; provided this situation is documented when a response is requested. Hustle reserves the right to require payment in advance, to withhold delivery of information until payment is received and to seek enforcement of charges. Non-binding estimates can be provided to the requesting parties. For an estimate, please email security@hustle.life with the requisite documentation and entitle the

subject “Estimate Request.” However, entities that fail to pay charges must serve process by the registered agent within the appropriate state and requests for expedited response will not be granted.

Criminal Legal Processes: Hustle will notify Customers upon receipt of criminal legal process seeking information about their accounts and/or data unless prohibited by law. Should Hustle receive any indefinite sealed legal process prohibiting notification of a Hustle Customer, including a national security letter gag, Hustle will invoke statutory procedures to have a judge review.

Hustle does not and will not provide User Content or data without a valid U.S. search warrant. Please note: If an emergency situation that presents a clear and present danger to life, or legal process prohibits notification; Hustle will notify Customer after emergency has ended, or once suppression order expires.

9. CHILDREN’S PRIVACY

Hustle does not knowingly collect or solicit any information from anyone under the age of 13 on this Service. In the event that we learn that we have inadvertently collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under 13, please contact us at privacy@hustle.com.

10. LINKS TO OTHER WEB SITES AND SERVICES

The Service may contain links to and from third-party websites of our business partners, advertisers, and social media sites and our users may post links to third-party websites. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for their policies. We strongly recommend that you read their privacy policies and terms and conditions of use to understand how they collect, use, and share information. We are not responsible for the privacy practices or the content on the websites of third-party sites.

11. HOW TO CONTACT US

If you have any questions about this Privacy Policy or the Service, please contact us at privacy@hustle.com.

12. CHANGES TO OUR PRIVACY POLICY

We may modify or update this Privacy Policy from time to time to reflect the changes in our business and practices, so you should review this page periodically. When we change the policy in a material manner, we will let you know and update the ‘last modified’ date at the bottom of this page. If you object to any changes, you may close your account. Continuing to use our Service after we publish changes to this Privacy Policy means that you are consenting to the changes.