PINDROP SUBSCRIPTION AGREEMENT FOR MARKETPLACES

Last Updated: December 15, 2025

This Pindrop Subscription Agreement for Marketplaces (the "**Agreement**") details the terms and conditions applicable to any Products or Services of Pindrop Security, Inc. ("**Pindrop**") that your company ("**Company**") obtains via an Approved Marketplace or the related Services that Company obtains from Pindrop via a Direct Order. By entering into a Order, Company agrees to be bound by the terms and conditions in this Agreement. If Company does not agree to the terms and conditions of this Agreement, Company shall not and does not have the right to use any Pindrop Property (as defined below). Pindrop agrees to be bound by the terms of this Agreement upon acceptance of the order(s) it enters into pursuant to the Approved Marketplace relevant to the Marketplace Order(s) or the Direct Orders, as applicable. Capitalized terms have the meaning given in this Agreement.

1. Definitions.

"Approved Marketplace" means the Google Cloud Marketplace, AWS Marketplace and Genesys' AppFoundry Marketplace and such other comparable marketplaces that Pindrop elects to offer its Products and Services from time to time.

"Authorized Geography" means the United States only with respect to where Company is authorized to (i) access and use a Product; and (ii) have the Product analyze calls made to Company Phone Number(s) intended for use by Company's customers also residing in the United States. For example, because Company is authorized to access and use the Product in the United States, then Company Phone Number(s) would be Company's Phone Number(s) that are intended for use by Company's United States-based customers as part of such customers conducting business with Company's United States-based business operations.

"Call" means a phone call made to the Company Phone Number that is processed by a Product.

"Call Heuristics" means the duration or frequency that a device's touch keys are held down (i.e., the frequency of a caller pressing a device's touch keys).

"Call Processing Data" means the data (excluding CPNI) obtained by or from a telecommunications network with respect to a Call that is generally used by telecommunication service providers for call routing purposes. Examples include data used to initiate, route, exchange and complete traffic that is internal to the network or networks during the call.

"Company Call Center Infrastructure" means Company's telephony solution with which Company will use a Product, including the Media Relay Services, as contemplated in the Agreement and/or Order.

"Company Call Data" means the data and information that are uploaded, transmitted, input or otherwise provided or made available by Company to Pindrop in connection with a Product. Examples of Company Call Data include the phone number from which a Call originates, audio (i.e., spoken content), signaling and call-related metadata from Company's telecommunications network (including the Telco Network Call Data) and Digital Signal for a given Call.

"Company Marketplace Agreement' means the written agreement between Company and the provider of the relevant Approved Marketplace pursuant to which Company orders a subscription to the Products and Services via such Approved Marketplace.

"Company Phone Number" means the then-current phone number(s) designated by Company, where calls made to that number(s) will be analyzed by a Product.

"Company Regulator" means any industry regulatory agency with supervisory authority over Company under applicable Laws.

"Confidential Information" means information designated as confidential or proprietary or that should be considered as confidential from its nature or from the circumstances surrounding its disclosure. The Pindrop Property is Confidential Information of Pindrop.

"Confirmed Fraud Call" means a Call that has been designated by Company through the user interface of the Product as being associated with fraudulent or suspicious activity during the course of Company's use of Pindrop's Product known as Pindrop® Protect or any subsequent Product(s) which also has the same functionality, as described in the applicable Documentation.

"Consortium Members" means Pindrop customers, government agencies, third party data providers, consumer agencies, credit lenders and other third parties that have themselves provided "fraudulent call data" to Pindrop or its subsidiaries. For clarity, unless expressly agreed otherwise by the parties in an Order, Pindrop customers with a subscription to Pindrop's authentication-only solutions (e.g., Pindrop® Passport) are not and do not become Consortium Members for purposes of this Agreement.

"CPNI" or "Customer Proprietary Network Information" means the data obtained by or from a telecommunications network with respect to a Call routed that relates to the quality, technical configuration, type, destination, location or amount of use of a telecommunications service about the calls placed from a particular phone number or is the type of call-related data that would customarily appear on the customer's bill who is purchasing the relevant telecommunications and interconnected VoIP services from a telecommunications services provider. Examples include the phone number of the calling party or called party, type of service the customer has ordered or the location of the customer or device.

"Digital Signal" means the digital signal used to transmit audio from the device and/or the telecommunications network.

"Direct Order" means an order that references this Agreement and entered into directly between Company and Pindrop applicable to PS that Pindrop will perform with respect to a Product covered under a Marketplace Order.

"Documentation" means any documentation, user guides and installation instructions provided by Pindrop to Company from time to time.

"DTMF" means the audio sound of the dual tone multiple frequency (i.e., the signal to the phone company when a caller presses a device's touch keys).

"Effective Date" means the date on which Company first enter into an Order for the Products or Services.

"Feedback" means all ideas, suggestions, or similar information that Company provides or otherwise make available to Pindrop or its subsidiaries with respect to the Products, Work Product or Services or any other Pindrop product or service offering.

"Fraudulent Call Data" means the following data for a Confirmed Fraud Call: (i) a phone number; (ii) the timestamp, duration, type of number and geography metadata; (iii) call type (e.g., mobile or VOIP); (iv) the Pindrop Score (i.e., the numerical risk score assigned to the Call); and (v) System Labels.

"Laws" means all laws, statutes, regulations and other types of government authority, including without limitation, the laws and regulations governing export control, unfair competition, anti-discrimination, false advertising, data privacy or data protection, and publicity.

"Marketplace Order" means an order or comparable document entered into through the standard offer and order process for the given Approved Marketplace that describes the Product(s) and/or related Services that Pindrop will provide to Company under this Agreement via such Approved Marketplace.

"Marketplace Provider" means the company who operates the Approved Marketplace (e.g., Google, AWS or Genesys).

"Media Relay Services" means the services purchased by Company from Verizon that enable the copying of the signal handler for a given call so that the call can be concurrently routed to multiple destinations, such as to the IVR for standard handling of that call (i.e., as if the Product were not in use by Company) and the Product for analysis and generation of the Pindrop Score.

"Order" means a Marketplace Order or Direct Order, as applicable.

"Outputs" means the data or information portion of a Product that are generated using Pindrop's proprietary technology and applicable to a Product's analysis of a particular Call (including by way of example only a Pindrop Score, System Labels, Proprietary Prints or audio recording of a Call, as applicable).

"Participants" means any persons, including Users, that participate in the use of, or in Company communications or transactions that are processed by, the Products delivered under this Agreement.

"Pindrop Database" means Pindrop's proprietary database that includes the Fraudulent Call Data as well as the same or similar data with respect to calls associated with fraudulent or suspicious activity provided by Consortium Members and other information derived from third party data providers and Pindrop's or its subsidiaries' own research efforts.

"Pindrop Property" has the meaning assigned in Section 6(f) (Pindrop Property) of this Agreement.

"Pindrop Score" means the scoring metrics, data or reasons for a scoring metric provided by Pindrop's proprietary processes, including statistical and audio models (e.g., phoneprints), intended to predict the likelihood of a phone transaction being fraudulent or suspicious or from someone other than an authenticated caller, as applicable depending on the features and functionality of a given Product.

"Pre-Ga Offering" means a new product or a potential new feature of functionality for an existing Product for which Company has a subscription that is provided in a Pindrop-managed lab environment and identified as "Beta," "Limited Availability," "Pre-Release" or similar designation or that is otherwise identified by Pindrop as unsupported.

"Product" means the Pindrop product(s) ordered by Company under an Order and the Pre-Ga Offerings.

"Professional Services" or "PS" means any implementation services (which may include installation, configuration, project management, process reviews and associated policy or procedure development, testing or go-live support), training or other optional services provided by Pindrop under an Order.

"Project Closure Milestone" means the date on which PS consisting of Pindrop's configuration and/or provisioning of the Product or any other mutually agreed-upon PS is deemed completed, as detailed in an Order.

"Proprietary Prints" means the numerical values generated by the Product that are a sequence of floating-point numbers, are not reversible into the original audio, are not composed of an audio wave file, and do not contain any actual recorded conversation. Examples of proprietary prints include: (i) Fakeprints (generic artifacts extracted to detect synthetic or recorded audio - not to identify a person); (ii) Toneprints (unique to device type and carrier – not person); (iii) Phoneprints (unique to device type, carrier and country location – not person; (iv) behavior heuristics (e.g., keypress patterns on device such as to help detect human vs robotic characteristics); and (v) voice features.

"Services" means PS or Support Services provided to Company under an Order.

"Subscription Term" means the time period that Company has the right to access and use a Product, as reflected in the relevant Order.

"Support Program Terms" means Pindrop's standard support and maintenance services program applicable to the Products and available here or such other terms a copy of which has been provided to Company, as updated and/or supplemented by Pindrop from time to time upon notice to Company.

"Support Services" means the support and maintenance services provided by Pindrop in connection with a given Product, as detailed in the Support Program Terms.

"Support Tools" means (i) software, web analytics tools or other technology used by Pindrop or its subsidiaries to (1) monitor, maintain or improve the performance, integrity or security of a Product; (2) identify portions of a Product that may require maintenance (including without limitation Errors that may require correction); (3) understand user behavior with a given Product (e.g., what feature or functionality is preferred), which may include the recording of a user's session while logged in to the Product; and (4) manage subscription-related metrics (e.g., quantity of Calls or expiration of a given Subscription Term); or (ii) cookies that are set on a user's browser and used by Pindrop or its subsidiaries for the purpose of identifying Users and Company's systems interacting with the Product or to logout a user after a period of inactivity, including the general location (e.g., city, state or country) of the IP addresses associated with users who login into and use a Product.

"System Label" means a label(s) automatically assigned to a Call (i) after it is dispositioned by an automated policy (as configured within the Product) or manually by a User as fraud/genuine and/or authenticated/non-authenticated; or (ii) to indicate it was answered or not answered during the course of being analyzed by a Product, in each case, as applicable based on the features and functionality of the Product.

"Telco Network Call Data" means, collectively, CPNI and Call Processing Data.

"User" means an individual who is authorized by Company to use a Product and who has been assigned by Company (or, when applicable, Pindrop or its subsidiaries at Company's request), a user identification number and password in to access such Product.

"Work Product" means any inventions, discoveries, software or other works of authorship (including, without limitation, configuration of a Product, accuracy reports and other documentation), and other proprietary materials or work product developed by or for Pindrop or its subsidiaries, alone or with others, in the course of Pindrop's performance of Services, including any and all related and underlying software, databases (including data models, structures, and non-specific data to Company contained therein), specifications, technology reports and documentation.

2. Engagement Model; Fees and Payments.

(a) Engagement Model. Except as expressly provided otherwise in this Agreement, (i) as it relates to Marketplace Orders, Company shall look solely to the Marketplace Provider with respect to Company's rights and obligations for the Products and Services (including payment of any applicable fees), as detailed in the Company Marketplace Agreement and Marketplace Order,;

and (ii) as it relates to Direct Orders, Company shall look solely to Pindrop with respect to Company's rights and obligations for the Products and Services (including payment of applicable fees) as detailed in this Agreement and the relevant Direct Order.

(b) Marketplace Orders – Description of Fees and Invoice Schedule. Company shall pay the fees for Products and Services in accordance with the applicable Company Marketplace Agreement and Marketplace Order.

(c) Direct Orders – Description of Fees and Invoice Schedule. Company shall pay Pindrop the fees for Services in accordance with the Direct Order. If an invoice schedule for Services is not specified in the Order, then fees for such Services will be invoiced and payable upon completion by Pindrop thereof. All fees will be invoiced and payable in U.S. Dollars and are due and payable to Pindrop within 30 days after the date of invoice to Company for such amounts (the "**Due Date**"). Company shall promptly reimburse Pindrop for any reasonable out-of-pocket expenses incurred by Pindrop in connection with providing PS to Company. All such expenses will be billed as incurred in accordance with Pindrop's travel and expense policies. Company shall pay all taxes, tariffs and transportation costs relating to, or incurred under, this Agreement or a Direct Order (including any sales, use, excise or value added taxes), exclusive of taxes based on or measured by Pindrop's net income, unless Company is exempt from the payment of such taxes. To the extent applicable, Company will provide to Pindrop any resale exemption certificate, direct pay permit or other exemption certificate or information reasonably requested by Pindrop. Company shall promptly notify Pindrop if any such exemption is subsequently revoked or modified. If Pindrop is required or permitted by applicable Law to charge and collect sales, use, excise, value-added or similar taxes (but excluding taxes based on or measured by Pindrop's net income) that are directly imposed on the purchase, lease or other transfer of taxable Products or Services for a consideration, Pindrop shall separately state such taxes on Company invoices along with other applicable related charges, including transportation and tariffs. Company shall promptly pay invoiced taxes. Notwithstanding the foregoing, the failure of Pindrop to properly designate all taxes on an invoice shall not relieve Company of its obligation to pay all such taxes. To the extent Pindrop fails to designate such taxes on an invoice, Company shall, upon notice and request by Pindrop, promptly pay or reimburse Pindrop for any taxes that are Company's responsibility under this Section. If Company fails to remit an undisputed portion of a payment by the applicable Due Date, Pindrop reserves the right to apply late charges at the lesser of (X) 1.5% per month of the overdue amount; or (Y) the maximum amount permitted under applicable Law. Disputes arising from invoices will be handled on a case by case basis. Company must notify Pindrop of any invoice dispute no later than the applicable Due Date or such invoice will be deemed approved and accepted by Company. Both parties will use their commercially reasonable efforts to assess and rectify, if applicable, discrepancies found within a disputed invoice as soon as commercially practicable.

3. General Pindrop Responsibilities.

(a) **Provision of Products and Services.** Pindrop and/or its subsidiaries will make the Products and Services available to Company (i) subject to the terms and conditions of this Agreement; and (ii) solely for lawful purposes and use.

(b) **Protection of Company Data.** During the term of this Agreement and for as long as Pindrop maintains Company's Confidential Information within the Pindrop-Controlled Systems, Pindrop will have and maintain the information security program and safeguards as detailed Exhibit C (Pindrop Information Security and BCP Programs).

(c) **BCP Program.** Pindrop will maintain and administer a Business Continuity Program ("**BCP**") for the Products, as detailed in Exhibit C (Pindrop Information Security and BCP Programs).

(d) **Compliance with Laws.** Pindrop represents and warrants that the Products and Services (including the manner in which Company Call Data is processed therein) will comply with applicable Laws. Pindrop shall not be in breach of this Section to the extent such non-compliance is based on or arises from Company's unauthorized use of the Products and/or Services or a breach of Company's obligations in this Agreement**.**

(e) **Pindrop Personnel**. Pindrop will be responsible for the performance of and compliance by its and its affiliates' personnel(including employees and contractors) with Pindrop's obligations under this Agreement and each Order (as applicable), except as otherwise specified in this Agreement. If Company determines, in its commercially reasonable judgment, that personnel assigned by Pindrop do not possess suitable knowledge or expertise or have violated Company's generally applicable working terms or conditions, Company may request that Pindrop replace such personnel within a reasonable period of time.

4. Use of Products and Services.

(a) **Subscriptions.** Unless otherwise provided in the Order, the Products and Services are purchased as subscriptions for the Subscription Term. Company agrees that its purchases are not contingent on Pindrop's delivery of any future functionality or features, or dependent on any oral or written comments made by Pindrop regarding future functionality or features.

(b) **Access to and Use of Products and Services.** Company has the right to access and use the applicable Products and Services subject to the terms of the applicable Order, this Agreement and the Documentation. The Product may contain certain Third-Party Software Components (defined below). Company's right to use the Third-Party Software Components is subject to the relevant third-party terms identified within the Product and/or the Product's associated Documentation applicable to each Third-Party Software Component, but only if and to the extent that Company's actual access and use of the Product requires Company to agree to different or new terms and conditions than those in this Agreement or any relevant Order (the "Third Party Terms"). For purposes of this Section, "Third-Party Software Components" means the third-party software bundled with or included the Product for which Pindrop has an obligation to pass-through the applicable open source or proprietary commercial software license terms directly to Company from the applicable third party licensor.

(c) **Company's General Responsibilities.** Company will (i) be responsible for its Users' compliance with this Agreement, the applicable Documentation and Orders; (ii) be responsible for the accuracy, quality and legality of Company Call Data, including as detailed in Section 8 (Company's Responsibility Statement) of this Agreement, and, with respect to the transmissions of Company Call Data via the Product, Company will also comply with Pindrop's current acceptable use policy available here; (iii) use commercially reasonable efforts to prevent unauthorized access to and use of the Products and Services, and notify Pindrop promptly of any such unauthorized access or use; (iv) use the Product(s) (including the Outputs) solely for security purposes (i.e., fraud detection and/or authentication), including with Company's own products or services based on the features and functionality enabled in a given Product and for no other purpose (e.g., not for credit or employment decisioning purposes or to determine a consumer's eligibility for credit or insurance, or for any other permissible purpose set forth in the FCRA (as defined below)); and (v) except as expressly provided otherwise in this Agreement, be solely responsible for, and agree to comply with, all applicable Laws with respect to Company's access and use of the Products and Services. For clarity, Pindrop is not a consumer reporting agency and none of the information provided through the Products constitutes a "consumer report", as such term is defined in the Fair Credit Reporting Act ("**FCRA**"), 15 U.S.C. § 1681 et seq.

(d) **Restrictions.** Company will not: (i) make any Pindrop Property available to anyone other than Company or its Users, or use any Pindrop Property for the benefit of anyone other than Company or Company's subsidiaries; (ii) sell, resell, sublicense, distribute, rent or lease the Pindrop Property in any manner (including without limitation in any service bureau or outsource offering); (iii) copy, modify or create derivative works of all or any portion of the Pindrop Property; (iv) except to the extent permitted by applicable Law, disassemble, reverse engineer or decompile all or any portion of the Pindrop Property in any manner; (v) frame or mirror any part of the Products, other than framing on Company's own intranets or otherwise for Company's own internal business purposes of as permitted in the Documentation; (vi) manually enter and/or import any Company Call Data into a Product that would or could violate Payment Card Industry Data Security Standard (PCI DSS), as amended from time to time, including by way of example only, a credit security validation (CSV) number and a credit card account number (the "**PCI Restriction**"); (vii) attempt to gain unauthorized access to the Products or related systems or networks, or permit direct or indirect access to or use of the Pindrop Property in a way that circumvents the terms of this Agreement or any other applicable security restrictions; (viii) access or use the Pindrop Property to (A) build a competitive product or service, (B) build a product or service using similar ideas, features, functions or graphics of the Pindrop Property, or (C) copy any ideas, features, functions or graphics of the Pindrop Property; or (ix) directly or indirectly authorize any third parties to do any of the foregoing. Any use of the Products in violation of this Agreement or the applicable Order or that in Pindrop's commercially reasonable business judgment threatens the security, integrity or availability of the Product to Pindrop's or its subsidiaries' customers, may result in immediate suspension of Company's access to the Product. However, Pindrop will use commercially reasonable efforts under the circumstances to provide Company with written notice (email is sufficient) and an opportunity to remedy such violation or threat prior to suspension. Further, if a breach occurs with respect to the Outputs, Pindrop reserves the right to require Company to delete and/or destroy the Outputs (as well as any derivative works, benchmarking or competing solution) in Company's possession or control.

(e) **Special Terms for Pre-Ga Offerings.** Pindrop may make Pre-GA Offerings available to Company from time to time. Pre-GA Offerings are subject to the same terms and conditions in this Agreement and each relevant Order, except as provided otherwise in this Section or an Order. Pre-GA Offerings are provided on an "as is" basis and are not included in the support obligations or in Pindrop's business continuity program, as detailed in Section 3(c) (BCP Program), and may be changed, suspended or discontinued by Pindrop at any time with prior notice to Company. Except as expressly indicated otherwise in a written notice from Pindrop or the Documentation for a given Pre-GA Offering, Company's access and use of a Pre-GA Offering is limited to Company's employees and the Authorized Geography, is solely for internal evaluation and/or testing purposes, and is subject to any additional terms identified and mutually agreed to by Pindrop and Company in writing, including geography or call traffic (i.e., "test" or production calls) restrictions. Either party may terminate Company's use of a Pre-GA Offering at any time with written notice to the other party.

(f) **Pindrop Pulse Warranty**. As part of a three (3) year subscription to the Pindrop® Pulse Technology™, and subject to Company's license to the complete Product Suite and the additional terms in the State of the Pindrop Pulse Warranty (available at

https//www.pindrop.com/pulse-deepfake-warranty-terms), Pindrop will provide Company the Pulse Warranty at no additional cost. Reimbursement for Company's Lost Funds is conditioned on Company's compliance with the terms of the Statement of the Pindrop Pulse Warranty. "Product Suite", "Pulse Warranty" and "Lost Funds" have the meanings given in the Statement of the Pindrop Pulse Warranty.

5. Confidentiality.

(a) **Use and Disclosure.** With respect to any Confidential Information a party receives ("**Receiving Party**") from the other party ("**Disclosing Party**"), the Receiving Party shall: (i) keep such information confidential; (ii) use the same degree of care for the Disclosing Party's Confidential Information that it uses for its own Confidential Information, but in no event less than reasonable care; (iii) not use the Confidential Information other than in connection with the performance of this Agreement and each Order; and (iv) not divulge the Confidential Information to any third party. Receiving Party agrees to use all reasonable steps to ensure that the Disclosing Party's Confidential Information is not disclosed by a Receiving Party Representative (defined below) in violation of this Section. Company also agrees that Company shall not disclose the results of benchmark tests or any other evaluation of any Pindrop Property to any third party without Pindrop's prior written approval. For purposes of this Section, "third party" excludes the Receiving Party or its affiliates employees, contractors, subcontractors attorneys, accountants or other professional advisors of the Receiving Party, as long as such representative (1) has a commercially reasonable need to know and access such Confidential Information in connection with the authorized purposes; and (2) is under contractual or fiduciary confidentiality obligations substantially equivalent to the terms and conditions of this Section (each a "**Receiving Party Representative**"). A Receiving Party is responsible for a breach by the Receiving Party Representative of the confidentiality obligations in this Agreement to same extent as the Receiving Party itself.

(b) **Exclusions.** Confidential Information shall not include information that: (i) is or becomes generally known or available to the public at large other than as a result of a breach by the Receiving Party of any obligation to the Disclosing Party; (ii) was known to the Receiving Party free of any obligation of confidence prior to disclosure by the Disclosing Party; (iii) is disclosed to the Receiving Party on a non-confidential basis by a third party who did not owe an obligation of confidence to the Disclosing Party; or (iv) is developed by the Receiving Party independently of and without reference to any part of the Confidential Information. Confidential Information shall not be deemed to be in the public domain or generally known or available to the public merely because any part of said information is embodied in general disclosures or because individual features, components or combinations thereof are now or become known to the public.

(c) **Limited Exceptions.** Confidential Information may be disclosed in response to a valid order by a court or other governmental body of the United States or any political subdivision thereof, as otherwise required by law, or as necessary to establish the rights of either party under this Agreement, provided that the party making such disclosure must provide written notice to the other party prior to such disclosure in order to provide the other party with a reasonable opportunity to obtain a protective order or otherwise protect the confidentiality of such information. During the term of this Agreement, the Receiving Party may publicize the existence of the relationship between Pindrop and Company in connection with the Products or Services being provided under Order(s) and Pindrop may list Company's name on Pindrop's standard customer lists.

6. Proprietary Rights and Other Licenses.

(a) **Use of Company Call Data.** Company grants Pindrop, its subsidiaries and applicable subcontractors a limited-term license to collect, use, record, host, transmit and process Company Call Data as necessary to provide, maintain and support the Product for Company in accordance with this Agreement, each Order and the applicable Documentation.

(b) **Company Use Rights.** Subject to the terms and conditions of this Agreement, Pindrop hereby grants to Company a limited, non-exclusive, non-transferable (except as expressly provided in this Agreement with respect to the entire agreement) right (i) during the applicable Order to access and use a Product solely within the Authorized Geography; (ii) during and after expiration of the applicable Subscription Term to retain and use the portion of the Outputs that are available via the outbound API feed(s) or standard export functionality from the Product solely for Company's internal business and recordkeeping purposes; and (iii) retain and use the portion of the Work Product available to Company in connection with or as part of the Services for Company's internal business purposes in connection with Company's use of the Product; provided that (A) the Outputs and such Work Product remain the Confidential Information of Pindrop and subject to the obligations of confidentiality and use restrictions set forth in this Agreement; and (B) Company shall not create any derivative works nor use the Outputs or such Work Product to create a competing solution. For clarity, to the extent Company Call Data (such as the phone number of a caller) is contained in an Output or such Work Product, nothing in this Section shall restrict Company's right to use Company's own Company Call Data in any manner.

(c) **Data Privacy Terms.** The additional data privacy terms and conditions in Exhibit A (Data Privacy Terms) of this Agreement apply.

(d) **Support Data and Product Optimization Uses.** Pindrop and its subsidiaries may use Support Tools. Notwithstanding anything to the contrary in this Agreement and subject to the use restrictions below, Company agrees that Pindrop and its subsidiaries can collect, analyze, retain and use the usage, statistical, caller phone number, metadata and other log data collected by Support Tools or Products (the "**Support Data**") to maintain, develop, manage, administer and improve Pindrop's and its subsidiaries' products and services, including the Products and Services and the AI Tools, applicable to such products and services (the "**Product Optimization Purposes**"). Except where Pindrop or its subsidiaries are using the Support Data for Company's sole benefit in its or their provision of the Products and Services to Company (such as to respond to trouble tickets), Pindrop and its subsidiaries will only use the Support Data for Product Optimization Purposes if the Support Data has been aggregated with other comparable data from other customers and then implemented by Pindrop or its subsidiaries as a general, customer-agnostic improvement to the general usability or efficacy of Pindrop's or its subsidiaries' products and services (i.e., in a manner that does not identify Company or any individual person within Company as the source of that data or any individual or phone number of an individual who called Company for the benefit of other customers). Company agrees that Pindrop's and its subsidiaries' right to retain and use the Support Data for Product Optimization Purposes shall survive any termination or expiration of this Agreement or any Orders. Company is responsible for disclosing to and obtaining consent from Company's Users to the collection and use of Support Data, as required by applicable Laws.

(e) **Pindrop Property.** Subject to the limited rights expressly granted by Pindrop under this Agreement, Pindrop and its subsidiaries and its and their licensors and third party providers reserve and retain and own all rights, title and interests in and to the Products (including Outputs and AI Tools), the Services (including Work Product), Documentation and all updates, upgrades, derivative works, modifications, conversions, improvements or the like made to each of the foregoing, together with all intellectual property rights embodied therein (collectively, the "**Pindrop Property**"). If Company Call Data (such as a caller's phone number) is contained in an Output or used by an AI Tool, nothing in this Section transfers or otherwise restricts Company's ownership in or right to use Company Call Data in any manner. Company agrees to retain and reproduce all copyright, trademark and other proprietary notices contained on or in the Pindrop Property as delivered to Company on all copies of such Pindrop Property and shall not seek to remove any such notices.

(f) **Company Property.** Subject to the limited rights expressly granted by Company under this Agreement or an Order, Company retains and owns all rights, title and interests in all intellectual property rights in and to the Company Call Data, Company Phone Number and Company Call Center Infrastructure.

(g) **Feedback.** Company may, at Company's sole election, provide Feedback to Pindrop or its subsidiaries to help identify ways in which Pindrop or its subsidiaries may improve or expand their product and service offerings for its customers. If provided, Company agrees to assign and hereby assigns to Pindrop all rights, title and interests in and to the Feedback.

(h) **AI Overview Terms.** Company understands that the nature of Pindrop's Products is to provide a probabilistic determination as to whether a call may be fraudulent, genuine or that the caller may be human or a machine, depending on which Products are in use by Company under this Agreement. As such, all Products have and will continue to use AI Tools (as defined in Exhibit D) in order to provide the core functionality of each such Product (such as a fraud risk score or a "liveness" score as to whether a caller may be human or machine). The additional terms and conditions in Exhibit D (AI Terms) shall apply to all AI Tools.

7. Implementation and Product-Specific Terms. The implementation-related and product-specific terms in Exhibit B (Implementation-Related Terms) shall apply, as applicable.

8. Company's Responsibility Statement. Company warrants, acknowledges and agrees that (i) Company will, on behalf of itself and on Pindrop's and its subsidiaries' behalf as Company's service provider(s), provide all required consumer notices and disclosures and, where required, secure consents in compliance with all applicable Laws with respect to the Outputs and Company Call Data (including Company's Personal Information and in relation to the locations where the Outputs and Company Call Data may be collected, stored and processed by Pindrop as a service provider or its service providers, each as set out in more detail in Exhibit A (Privacy Terms)); and (ii) Company will have and maintain privacy policies and terms and conditions with Company's Participants that are compliant with its obligations and applicable Laws and permit the use and sharing of information processed, analyzed or created by a Product (including the creation of Outputs) and/or contributed to the Pindrop Database as contemplated in Agreement or an Order (collectively, the responsibilities under (i) and (ii) shall be referred to as the "**Customer Commitments**"). If Company is a "Financial Institution" under the Gramm-Leach-Bliley Act (the "**GLBA**"), then (A) Company further warrants that Company's Customer Commitments are also compliant with Company's obligations as a Financial Institution under the GLBA; and (B) for the duration of Company's access to and use of the Product(s) and Services, Company hereby appoints Pindrop as a special agent for Company with limited authority to perform functions inherent in the Products and Services as necessary for the purposes of Company's fraud prevention and enhancing security in connection with customer transactions. The limited authority

granted in subsection (B) above is the "Limited Authority Agency." Other than the foregoing appointment in (B), Pindrop has no right, power, or authority to bind Company or create any obligation or responsibility on Company's behalf beyond the Limited Authority Agency. If Pindrop, in its good faith judgment, believes that the Products are being used in a manner that is not compliant with applicable Laws or that such use could result in noncompliance with applicable Laws and/or such use could subject Company or Pindrop to a claim for liability for noncompliance, or otherwise harm Pindrop or its reputation, Pindrop reserves the right to modify its Products or Services accessed or used by Company as deemed reasonably necessary to address such noncompliance. Company agrees to cooperate with Pindrop to the extent reasonably necessary to effectuate such modifications.

9. Limited Warranties. EXCEPT AS PROVIDED OTHERWISE IN THIS AGREEMENT , TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PINDROP PROPERTY IS PROVIDED TO COMPANY "AS IS," AND PINDROP AND ITS SUBSDIARIES, AND ITS AND THEIR LICENSORS AND THIRD PARTY SERVICE PROVIDERS DISCLAIM ANY AND ALL OTHER PROMISES, REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, QUIET ENJOYMENT, SYSTEM INTEGRATION AND/OR DATA ACCURACY. PINDROP, ON BEHALF OF ITSELF AND SUBSIDIARIES AND ITS AND THEIR LICENSORS AND THIRD PARTY SERVICE PROVIDERS, DOES NOT WARRANT THAT THE PINDROP PROPERTY WILL MEET COMPANY'S REQUIREMENTS, THAT THE OPERATION OR USE OF THE FOREGOING WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE CORRECTED. COMPANY ACKNOWLEDGES AND AGREES THAT THE DISCLAIMERS, LIMITATIONS AND EXCLUSIONS OF LIABILITY SET FORTH IN THIS AGREEMENT FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES, AND THAT, ABSENT SUCH DISCLAIMERS, LIMITATIONS AND EXCLUSIONS, THE TERMS OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THE ECONOMIC TERMS, WOULD BE SUBSTANTIALLY DIFFERENT.

10. Limitation of Liability; Consequential Damages Waiver.

(a) **Consequential Damages Waiver** IN NO EVENT SHALL EITHER PARTY OR ITS SUBSIDIARIES BE LIABLE TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER BASED ON DAMAGES, LOSSES OR COSTS INCURRED AS A RESULT OF LOSS OF TIME, LOSS OR CORRUPTION OF APPLICATION OR DATA, LOSS OF PRODUCT OR REVENUE, OR LOSS OF USE OF THE PRODUCTS, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT PRODUCT LIABILITY, OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OF ANY SUCH DAMAGES IN ADVANCE.

(b) **Liability for Direct Damages.** THE MAXIMUM AGGREGATE LIABILITY OF EACH PARTY OR ITS SUBSIDIARIES FOR DAMAGES TO THE OTHER ARISING FROM OR RELATED TO THIS AGREEMENT OR ANY PINDROP PROPERTY, WHETHER FOR BREACH OF CONTRACT OR WARRANTY, STRICT LIABILITY, NEGLIGENCE OR OTHERWISE, SHALL NOT:

(i) FOR PINDROP, EXCEED TWO TIMES THE FEES PAID TO PINDROP DURING THE PRECEDING 12 MONTHS FOR THE PRODUCT, WORK PRODUCT OR SERVICES UNDER THE ORDER GIVING RISE TO SUCH LIABILITY; AND

(ii) FOR COMPANY, EXCEED TWO TIMES THE FEES PAID OR PAYABLE BY COMPANY TO PINDROP DURING THE PRECEDING 12 MONTHS FOR THE PRODUCT, WORK PRODUCT OR SERVICES UNDER THE ORDER GIVING RISE TO SUCH LIABILITY.

(c) **Exclusions**.

(i) Liability for (1) infringement and misappropriation by one party of the other party's intellectual property rights; (2) a breach by a party of its confidentiality obligations under this Agreement; (3) fulfillment by Pindrop of its obligations and liabilities pursuant to Section 11(a) (Pindrop Coverage for Third Party Claims) and, as a Responsible Party, pursuant to Section 11(c) (Procedural Requirements for Third Party Claims); (4) fulfillment by Company of Company's obligations and liabilities pursuant to Section 11(b) (Company Coverage for Third Party Claims) and, as a Responsible Party, pursuant to Section 11(c) (Procedural Requirements for Third Party Claims); and (5) a party's liability for any gross negligence or willful misconduct, shall each be excluded from the limitations on liability in Sections 10(a) (Consequential Damages Waiver) and 10(b) (Liability for Direct Damages). Responsible Party has the meaning assigned in Section 11(c) (Procedural Requirements for Third Party Claims).

(ii) Liability for a breach (i) by Company of Section 8 (Company Responsibility Statement) and the PCI Restriction; and (ii) liability for any death, personal injury or damage to tangible property resulting from the acts and omissions of a party (except to

the extent such damage or injury was caused by the other party, its employees or representatives), shall each be excluded from the limitations of liability in Section 10(b) (Liability for Direct Damages) .

11. Responsibility for Third Party Claims.

(a) **Pindrop Coverage for Third Party Claims.** Pindrop agrees, at its expense, to defend, indemnify and hold harmless Company from and against any and all third party claims, actions or demands and legal proceedings, liabilities, damages, losses, and judgments or authorized settlements, and reasonable costs and expenses as incurred, including without limitation attorneys' fees, arising from (A) Pindrop's failure to comply with its information security safeguards for Personal Data expressly set forth this Agreement where such failure results in a Security Breach (as defined in Exhibit B (Pindrop Information Security and BCP Programs); (B) Pindrop's breach of Section 3(d) (Compliance with Laws) of this Agreement; or (C) where the third party alleges that a Product furnished to Company and used within the scope of and in compliance with this Agreement infringes the intellectual property rights of a third party. Pindrop is not responsible under this Section for any infringement arising out of or related to: (I) modification of a Product by anyone other than Pindrop, where the Product would not infringe except for that modification; (II) any combination of the Product with other software, hardware, processes or materials not provided by Pindrop, where the Product would not infringe except for such combination; (III) Company's use of a version of the Product other than the most current release of the Products if infringement would have been avoided by use of the current release (but only if Pindrop has supplied Company with the most current release at no additional fee); or (IV) Company Call Data, where the Product would not infringe except for Company Call Data. If a Product is held or believed by Pindrop to infringe (and none of the exclusive above apply), Pindrop may, at its sole option and expense, elect to: (w) modify the Product so that it is non-infringing; (x) replace the Product with non-infringing products which are functionally equivalent or superior in performance; (y) obtain a license for Company to continue to use and access the Product as provided in the Order; or (z) terminate the license for the infringing Product and refund any prepaid but unused license fees paid for such Product under the impacted Order. THE RIGHTS GRANTED TO COMPANY UNDER THIS SECTION 11(a) ARE COMPANY'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF INFRINGEMENT OR MISAPPROPRIATION RELATED TO THE PRODUCTS AND THE THIRD PARTY CLAIMS DESCRIBED IN THIS SECTION 11(a).

(b) **Company Coverage for Third Party Claims.** Company agrees, at Company's expense, to defend, indemnify, and hold harmless Pindrop and its subsidiaries (each a "**Pindrop Party**") from and against any and all third party claims, actions, demands and legal proceedings, liabilities, damages, losses, and judgments or authorized settlements, and reasonable costs and expenses as incurred, including without limitation attorneys' fees, arising out of or in connection with any alleged or actual breach or violation of (i) Section 8 (Company Responsibility Statement), (ii) other applicable Laws for which Company is responsible under this Agreement in connection with Company's use of or access to the Products or Services by Company and any of Participants, including the collection, processing, analysis, creation, storage and retention of Company Call Data and Outputs; and (iii) the PCI Restriction.

(c) **Procedural Requirements for Third Party Claims.** For each party to be responsible for its indemnification obligations under Sections 11(a) (Pindrop Coverage for Third Party Claims) or 11(b) (Company Coverage for Third Party Claims), as applicable (the "**Responsible Party**"), the other party (the "**Covered Party**") shall (i) promptly notify the Responsible Party in writing of its receipt of notice of any claim or when it discovers facts on which the Covered Party intends to base a request for indemnification under such Section(s) of this Agreement (each a "**Claim Notice**"); (ii) afford the Responsible Party the choice to control the defense and all related settlement negotiations of such claim; provided that the Covered Party can participate at its own expense; and (iii) provide the Responsible Party with reasonable assistance, information and authority necessary to fulfill its obligations under Sections 11(a) or 11(b) above. Each party, as a Responsible Party, agrees to keep the Covered Party reasonably informed as to the status of the Responsible Party's efforts in connection with the defense or settlement of claims on behalf of the Covered Party and reasonably consult with the Covered Party (or the Covered Party's counsel) concerning such efforts.

Notwithstanding anything to the contrary in Section 11(c)(i), a Covered Party's failure to provide a Claim Notice does not relieve the Responsible Party of its liability to the Covered Party under Sections 11(a) or 11(b), as applicable, unless such delay materially prejudices the Responsible Party's defense or the scope of the Responsible Party's liability for the applicable third party claim.

Notwithstanding anything to the contrary in Section 11(c)(ii), the following apply:

(A) The Responsible Party agrees it will not, without the Covered Party's written approval, make any admission of facts that expose the Covered Party to any liability, require the Covered Party to take or cease to take any action (including without limitation any requirement to make payments), or expose the Covered Party to other claims that are not covered by the obligations for the applicable claim under Section 11. However, if the Responsible Party is required by applicable Law to make an admission, the Responsible Party may proceed in making such admission without the Covered Party's prior approval; provided the Responsible

Party provides written notice to the Covered Party with a reasonable opportunity to obtain a protective order or otherwise address such requirement with the appropriate authority.

(B) If the Responsible Party fails to respond to a Claim Notice or refuses to assume the defense of a claim tendered in good faith within 10 days of its receipt of the Claim Notice with respect to a claim for which it is seeking indemnification under this Section 10, then the Covered Party may proceed to defend or otherwise settle the claim as the Covered Party deems reasonably appropriate and the Responsible Party agrees to reimburse the Covered Party with respect to all defense costs, including but not limited to reasonable attorneys' fees and expenses or damages incurred with respect to such claim, as incurred.

12. Term and Termination.

(a) **Term of Agreement.** The term of this Agreement shall commence on the Effective Date and continue for the duration of the initial Order ("**Initial Term**"), unless terminated sooner. This Agreement automatically renews annually thereafter for additional 3 year periods unless one party provides the other party no less than 60 days written notice prior to the expiration of the then-current year (each a "**Renewal Term**" and together, the Initial Term and Renewal Term are the "**Term**"). This Agreement remains binding in full force and effect and continues to apply to any Orders that have not terminated or expired as of the effective date of termination of this Agreement until those Order(s) terminate or expire according to its terms . For clarity, a notice of non-renewal of this Agreement does not in any way modify, impact the validity of, or terminate any existing Orders

(b) **Mutual Rights of Termination.** Either party to this Agreement may terminate this Agreement or a Order if the other party materially breaches any section of this Agreement or a Order and fails to cure such breach upon 30 days prior written notice by the non-breaching party (the "**Cure Period**") specifying the nature of the breach and the reasonable actions required to cure the breach, provided, however, that if the breach does not involve payment of amounts to Pindrop and is of a nature that can be cured but not within the Cure Period, and the breaching party has commenced significant efforts to cure the breach within the Cure Period, this Agreement or Order will not terminate so long as the breaching party continues to diligently pursue the completion of such cure.

(c) **For Cause Termination.** Where Pindrop rightfully terminates this Agreement pursuant to Section 12(b) (Mutual Rights of Termination), Company acknowledges and agrees that Pindrop can also immediately terminate the impacted Order(s) upon written notice to Company without liability of any kind or nature incurred by either Pindrop. Where Company rightfully terminates this Agreement pursuant to Section 12(b) (Mutual Rights of Termination), any corresponding rights Company may have to terminate the impacted Order(s) shall be pursuant to the terms in this Agreement and such Order(s).

(d) **Termination for Change in Legal Requirements.** Company may terminate this Agreement) or any Order upon written notice to Pindrop if, after the Effective Date of this Agreement, an applicable Law becomes effective prohibiting Company from using or being engaged in the use of the Product(s) with its customers or that materially impairs the ability or power of Company to use the Product(s) in compliance with any new applicable Law, either through Pindrop or otherwise; provided that the parties have met and discussed in good faith the impact of the new applicable Law on the Product(s), Company has provided written notice to Pindrop detailing its concerns with Pindrop's plan or activities to address such change and Company is not reasonably satisfied with Pindrop's proposed plan or activities for addressing such change.

(e) Obligations Upon Termination. Upon the expiration or termination of this Agreement or an Order for any reason, all rights and licenses granted to Company under this Agreement and all impacted Orders shall immediately terminate and all impacted Pindrop Property shall, at Pindrop's sole option, be returned to Pindrop or destroyed by Company. Further, upon request by a Disclosing Party, a Receiving Party agrees to (i) destroy the Disclosing Party's Confidential Information in its possession or control; and (ii) confirm in writing to the Disclosing Party that it has complied with the destruction instructions with respect to the Disclosing Party's Confidential Information. However, with respect to any Confidential Information (1) in the Receiving Party's or its subcontractors' archive (including legal archives and business records generated in the delivery and support of the Products and Services), back-up or other comparable systems or servers; (2) expressly authorized in this Agreement or Order; or (3) retained to comply with litigation holds or applicable Law, such Confidential Information is only required to be destroyed in accordance with the Receiving Party's and its subcontractors' then-current data retention policies, litigation hold or applicable Law, whichever is the longest of the retention requirements. An Order may specify additional or different obligations upon termination for a given Product. Company understands and agrees that Pindrop has no obligation to save or otherwise make all or any portion of the Outputs available after the effective termination date of an Order. The terms in this Section 12(e), all defined terms, terms which expressly survive expiration or termination and the rights and obligations contained in Sections 2 (Engagement Model), 3(b) (Protection of Company Call Data), 5 (Confidentiality), 6(d) (Support Terms), 6(f) (Pindrop Property), 6(g) (Company Property), 6(h) (Feedback), 9 (Limited Warranties), 10 (Limitation of Liability; Consequential Damages Waiver), 11 (Responsibility for Third Party Claims), 13 (Audits), and 14 (General) shall survive any expiration or termination of this Agreement and any Orders.

13. Audits. During the term of this Agreement and for a period of 6 months after the Term, upon reasonable prior written notice

to the other party (email is sufficient), a party to this Agreement (an "**Auditing Party**") shall have the right, upon reasonable advance written notice to the other party, at its expense, to conduct (or have a third party conduct) an audit, assessment, examination or review of relevant documentation, materials or systems of the other party (the "**Audited Party**") for the sole purpose of assessing compliance by the Audited Party with the terms and conditions of this Agreement and any usage rights applicable to the Pindrop Property relevant to each Order (e.g., quantity of Calls included with the Subscription Term). The Audited Party shall reasonably cooperate with any such request by providing reasonable access to knowledgeable personnel, systems, documentation, and other reasonably requested information. Company acknowledges and agree there may be restrictions on Company's ability to conduct audits on Pindrop's subcontractors.

Audits shall not be conducted more than once per year (unless a material non-compliance is detected in which case an additional audit may be performed to verify that any agreed to corrective actions have been taken). Additionally, audits must be conducted during normal business hours and in a manner not to unreasonably disrupt the Audited Party's day to day business Any site visit at the Audited Party and/or audit of the Audited Party's procedures, systems and equipment shall be subject to such reasonable policies and practices of the Audited Party that are in effect for any site visits and audits of the Audited Party to maintain the security of the Audited Party's site, its systems and equipment and to protect the confidentiality of information which is proprietary and confidential to the Audited Party and that of any of its other customers or vendors. An Audited Party will not be required to give access to or disclose any confidential information of a third party or any attorney-client privileged information. The Auditing Party has no obligation to share any of its audit results with the Audited Party. However, the results of any audit shall constitute Confidential Information of both parties, and in all cases, be subject to the confidentiality obligations under this Agreement with respect to Confidential Information contained in the audit report(s).

14. General.

(a) **Export Compliance.** The Pindrop Property and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not on any U.S. government denied-party list. Company will not permit any User to access or use any Pindrop Property in a U.S.-embargoed country or region (currently Cuba, Iran, North Korea, Syria or Crimea) or in violation of any U.S. export law or regulation or other equivalent laws of other jurisdictions, as applicable.

(b) **Governing Law; Jurisdiction and Attorneys' Fees.** This Agreement will be governed by and construed in accordance with the laws of the State of Delaware, without regard to its conflict of law provisions. With respect to any legal disputes between Company and Pindrop arising out of or related to this Agreement, Company and Pindrop irrevocably consent to the exclusive personal jurisdiction of the federal courts located in Delaware or, if the Federal courts do not have jurisdiction, in the Superior Court of the State of Delaware, and any appellate court from any such state or Federal court. In the event of any dispute arising out of or related to this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees and costs.

(c) **Drafting.** The section headings appearing in this Agreement are inserted only as a matter of convenience and in no way define, limit, construe or describe the scope or extent of such section or in any way effect such section. In this Agreement, words importing the singular number include the plural and vice versa and words importing gender include all genders.

(d) **Notices.** All notices permitted or required under this Agreement shall be in writing and shall be delivered as follows with notice deemed given as indicated (i) by personal delivery when delivered personally; (ii) by commercially established courier service upon delivery or, if the courier attempted delivery on a normal business day and delivery was not accepted, upon attempted delivery; or (iii) by certified or registered mail, return receipt requested, 10 days after deposit in the mail. Notice will be sent to the parties at the addresses as each party shall notify the other of in writing. Pindrop's notice information is as follows: Pindrop Security, Inc.**, Attn: Legal Department**, 1115 Howell Mill Road NW, Suite 700, Atlanta, GA 30318, with copy to: generalcounsel@pindrop.com.

(e) **Waivers; Severability.** Neither party shall by mere lapse of time without giving notice or taking other action be deemed to have waived any breach by the other party of any of the provisions of this Agreement. Further, the waiver by either party of a particular breach of this Agreement by the other party shall not be construed as, or constitute, a continuing waiver of such breach, or of other breaches of the same or other provisions of this Agreement. If any provision of this Agreement shall be held illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, the validity of the remaining portions or provisions hereof shall not be affected.

(f) **Joint and Several Liability for Subsidiaries.** Each of Company's subsidiaries that utilizes the Products and Services under this Agreement shall be jointly and severally liable with Company for all obligations and liabilities arising under this Agreement

provided that the aggregate liability of Company and Company's subsidiaries shall not exceed the limitations of liability set forth in this Agreement. Company warrants that Company has the authority to bind its subsidiaries to the terms of this Agreement.

(g) Force Majeure. Except for the payment of money due or payable, neither party is liable for any failure or delay in performance under this Agreement which might be due to strikes, shortages, riots, insurrection, fires, flood, storm, other weather conditions, explosion, acts of God, war, government action, inability to obtain delivery of parts, supplies or labor, labor conditions (including strikes, lockouts or other industrial disturbances), earthquakes, riots or acts of terrorism, epidemic, pandemic or any other cause which is beyond the reasonable control of such party (each a "force majeure event"). The occurrence of a force majeure event shall not relieve Pindrop of its obligation to implement its disaster recovery plan or provide disaster recovery services with respect to an impacted Product, as contemplated in Section 11 (BCP Program) of Exhibit C (Pindrop Information Security and BCP Program) attached.

(h) **Assignment.** Each party may, with prior written notice to the other party and conditioned upon the contemporaneous corresponding assignment of any applicable Order(s), assign this Agreement and such Order(s) to any third party who succeeds to substantially all of that party's assets and business related to the Products covered under this Agreement by merger or purchase, provided that the assignee assumes this Agreement by an instrument in writing. Except as authorized in the preceding sentence, this Agreement, and any Order(s) entered into under this Agreement, may not be assigned or transferred by either party without the prior written consent of the other party. If Company is a financial institution under the GLBA and Company's assignee is not, then (i) Company must disclose that fact to Pindrop in its written notice of assignment; and (ii) Pindrop reserves the right, in its discretion, to modify any Products and Services accessed or used by such assignee, including by way of example only, disabling features or functionality in the Products or Services or as otherwise deemed reasonably necessary to comply with applicable Laws. Notwithstanding the foregoing, if the assignee of Pindrop is unacceptable to Company in its Company's good faith judgment for any legal or regulatory reason(s) or is unable to provide reasonable assurances that it has the financial, technical, or operational resources to fulfill its obligations under this Agreement: (A) Company may terminate this Agreement upon written notice to Pindrop within 1 month of receipt of Pindrop's notice of such change of control; and (B) in the event of any such termination, Pindrop will promptly refund to Company all prepaid, unused fees for any full year(s) of the Subscription Term remaining under the impacted Order(s) (i.e., not for the then-current year of the Subscription Term).

(i) **Entire Agreement.** This Agreement (i) is the complete agreement between the parties with respect to the subject matter hereof and supersedes any and all prior agreements and understandings; and (ii) unless expressly authorized otherwise in this Agreement, may be amended only in a writing that refers to this Agreement and is signed by both parties. The parties are independent contractors. Except as expressly agreed by the parties, neither party will be deemed to be an employee, agent, partner or legal representative of the other for any purpose and neither will have any right, power or authority to create any obligation or responsibility on behalf of the other. To the extent of any conflict between an Marketplace Order or Direct Order (as applicable)and this Agreement, unless expressly provided otherwise in a Marketplace Order or Direct Order (as applicable), the following shall be the order of priority for control: (i) the Marketplace Order or Direct Order; and (ii) the Agreement. To the extent of any conflict between this Agreement and the Company Marketplace Agreement with respect to the Pindrop Property or Pindrop's Confidential Information, this Agreement shall control.

(j) **Injunctive Relief.** Notwithstanding any other provision of this Agreement, any violation by either party to this Agreement of the other party's intellectual property or proprietary rights will cause irreparable damage for which recovery of money damages would be inadequate, and the aggrieved party will therefore be entitled to seek timely injunctive relief to protect such party's rights, without the need to post bond.

(k) **Limited Right to Modify Terms.** If there is a change in any applicable Law, litigation or the regulatory landscape which affects this Agreement, or the activities of either party under this Agreement, and a party reasonably believes in good faith that the change will have a substantial adverse effect on that party's rights or obligations under this Agreement, then such party may, upon written notice, require the other party to enter into good faith negotiations to renegotiate the terms of this Agreement, with such notice providing reasonable detail as to the nature of any proposed modification.

****

Exhibit A - Data Privacy Terms

1. Definitions. In the event of a conflict between this definition and the definition of an applicable term under relevant Data Protection Law (defined below), the definition under the relevant Data Protection Law shall govern.

(a) "Aggregate Data" means information that relates to a group or category of individuals, from which individual identities have been removed, that is not linked or reasonably linkable to any individual or household, including via a device and "Aggregated" shall refer to the process to make any data Aggregated Data.

(b) Controller" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes similar terms under Data Protection Laws, such as terms "Business" and "Third Party," as context requires.

(c) "Data Protection Law(s)" means any applicable state or federal Laws for the protection, privacy and/or processing of Personal Data, including any amendment or re-enactment of the foregoing, to which Company or Pindrop are subject.

(d) "Deidentified Data" means information that cannot reasonably identify, be related to, describe, be capable of being associated with, or linked, directly or indirectly, to a particular individual, and "Deidentified" shall refer to the process to make any information Deidentified Data.

(e) "Personal Data" means any information that (i) identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device; or (ii) is made available to Pindrop by Company or on Company's behalf in connection with the Products and Services that Data Protection Laws define as "personal data," "personal information," "personally identifiable information" or similar term.

(f) "Process", "Processing", or "Processed" means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether automated or not, not, such as, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(g) "Processing Purpose" means the purpose for which Pindrop is Processing Personal Data as set forth in Section 2(b) of this Exhibit A and shall also be deemed to mean a Business Purpose.

(h) "Processor", means an entity that Processes Personal Data on behalf of another entity. "Processor" includes similar terms under Data Protection Laws, such as the term "Service Provider," as context requires. The terms "Business", "Business Purpose", "sell" (and its cognates), "share" (and its cognates) and "Third Party" will have the meaning as ascribed to it or to a similar term under applicable Data Protection Laws.

2. Processing Purpose. With respect to Pindrop's provision of the Products and Services to Company pursuant to this Agreement and the related Order(s) (the "**Relevant Agreements**"):

(a) As between Pindrop and Company, Pindrop is a Service Provider or Processor (as applicable), with respect to any Personal Data that Pindrop Processes, on Company's behalf, pursuant to this Agreement;

(b) Company has disclosed Personal Data to Pindrop and its affiliates for the following Processing Purposes: (1) detecting security incidents and/or utilization by a caller of a non-human voice, and protecting against malicious, deceptive, fraudulent or illegal activity (including, in each case, populating the Pindrop Database with Fraudulent Call Data); and (2) assisting in the authentication of Company's callers , as well as is reasonably necessary to support any other valid Processing Purposes that are part of the Products or Services so long as they are agreed to by the parties to this Agreement, including and subject to restrictions on use such as those applicable to Fraudulent Call Data;

(c) Company and Pindrop acknowledge and confirm any disclosure of Personal Data pursuant to this Agreement is exclusively for the provision of the Products and Services under this Agreement and that Pindrop does not receive any of Personal Data as monetary or other valuable consideration for any Products, Services or other items provided under this Agreement; and

(d) Company hereby instructs and authorizes Pindrop to Process Personal Data in connection with Pindrop's performance and exercise of its obligations and rights under this Agreement as set forth in Section 3 (Permitted Use) of this Exhibit. Any additional or alternate instructions must be mutually agreed upon in writing.

3. Permitted Use. Pindrop will only collect, use, retain, disclose and otherwise Process Personal Data solely: (i) for the Processing Purposes described above and its performance of this Agreement, including in support of Pindrop's and its affiliates internal operations as necessary to the provision of the Products and Services for Company, (ii) on Company's behalf and in accordance with Company's documented, written instructions; (iii) for its internal use to build or improve the quality of the Products and Services, provided that such use is specifically authorized in this Agreement

and Pindrop will not use the Personal Data to perform services on behalf of another person; or (iv) as otherwise necessary for compliance with applicable Laws. Pindrop will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of Personal Data and are subject to a duty of confidentiality with respect to Personal Data.

For clarity, Pindrop may retain use or otherwise Process certain Personal Data (and combine it with Personal Data from other clients) as reasonably necessary to detect data security incidents, or protect against fraudulent or illegal activity (e.g., as part of the Pindrop Database).

4. Subprocessors and Subcontractors. Company agrees and authorizes Pindrop to disclose Personal Data to, and permit the Processing of Personal Data by, its Subprocessors used to deliver and perform its obligations under this Agreement, subject to Pindrop's obligations hereunder and Data Protection Laws. A copy of Pindrop's current Subprocessors is available upon request. Pursuant and subject to Section 9 (Vendor Management Program) of Exhibit B (Pindrop Information Security and BCP Programs), Pindrop shall (i) upon request, provide Company with reasonable details of the Processing to be undertaken by any Subprocessor, (ii) conduct due diligence on the Subprocessor in order to ensure reasonable privacy and security measures are in place designed to protect Personal Data consistent with Data Protection Laws and the Agreement; and (iii) enter into a written agreement with each Subprocessor that Processes Personal Data that includes obligations to protect the confidentiality of such Personal Data and that is no more permissive on the processing of Personal Data than the limitations and restrictions imposed on Pindrop under the Agreement. Pindrop will be responsible and liable for the performance and actions of its Subprocessors that, if performed by Pindrop, will be deemed a breach the terms of the Agreement. Pindrop will provide Company with not less than 60 days prior written notice of any new Subprocessor prior to providing the new Subprocessor with Personal Data or access thereto. Pindrop will provide Company with 30 days to object to the changed Subprocessor, calculated from the date Pindrop notified Company in writing. If Company objects to a new Subprocessor within that 30 day period, Pindrop will not provide the Subprocessor with Personal Data or access thereto, and Pindrop will use reasonable efforts to adjust the Products and/or Services or recommend a commercially reasonable change to Company's use of the Products or Services to avoid Processing of Personal Data by the objected-to Subprocessor without adversely impacting the provision of the Products and Services to Company. If Pindrop, at its discretion, is unable to do either of the foregoing, Pindrop shall notify Company of such determination and Company may, in its sole discretion, terminate the Product(s) and/or Order(s) involving the objected-to Subprocessor on 30 days prior written notice to Pindrop. In this event, Company will not be entitled to a refund of any fees paid.

5. Restrictions. Pindrop will not (i) sell or share Personal Data in violation of Data Protection Laws; (ii) collect, retain, use, disclose or otherwise Process Personal Data for any purpose other than for the Processing Purpose, which, for the avoidance of doubt, also prohibits Pindrop from disclosing Personal Data to unauthorized third parties or for any other commercial purpose; or (iii) engaging in any targeted advertising or profiling. Pindrop certifies that it understands and will comply with the foregoing restrictions set forth in this paragraph.

6. Deidentified Data and Aggregated Data. Company acknowledges and agrees that (a) Pindrop and its affiliates may use Deidentified Data and Aggregate Data derived from the Products and Services, and general Product Optimization Purposes. Pindrop and its affiliates may also, during and after the Term , use, maintain, and disclose Deidentified Data and Aggregate Data for their own product improvement and general purposes. However, Pindrop agrees that it and its subsidiaries will not identify Company or otherwise disclose Company as the source of any such Deidentified Data or Aggregate Data in connection with any general use purpose. Pindrop further agrees it will not make any attempt to (1) re-identify the Deidentified Data; or (2) otherwise attempt to create or derive any Personal Data from such Deidentified Data or Aggregate Data, in each case without Company's express written permission.

7. Audit. Company shall have the right to audit Pindrop's Processing of Personal Data and Pindrop's compliance with this Exhibit A in accordance with Section 13 (Audits) of the main body of the Agreement. Any report, documents, information, or recorded provided to Company or created pursuant to this Section 7 shall be considered Pindrop Confidential Information.

8. Duration of Processing. Pindrop will only Process Personal Data for the duration of this Agreement and as otherwise allowed under this Agreement or permitted under applicable Law. Unless retention of Personal Data is otherwise permitted under this Agreement or required under Data Protection Laws, upon the termination or expiration of this Agreement for any reason, Pindrop will, at Company's choice, return to Company or securely destroy all Personal Data as soon as practicable, but no later than 90 days from such termination or expiration. Upon Company's request, Pindrop shall provide a certificate of deletion certifying that Pindrop has deleted or returned all Personal Data, as applicable. If Pindrop is obliged to retain Personal Data after termination or expiration of this Agreement to comply with a legal obligation to which it is subject, Pindrop will: (i) inform Company thereof; (ii) protect the confidentiality of the Personal Data in its possession; and (iii) no longer actively Process Personal Data.

9. Data Subject Requests. If Pindrop receives a complaint, dispute, or request from a data subject to exercise such data subject's rights under Data Protection Laws, and Pindrop is able to confirm that such request relates to Company, Pindrop will promptly notify Company of such data subject request, and in any event within 5 business days, or as soon as commercially reasonable, following Pindrop's confirmation. Taking into account the nature of Pindrop's Processing of Personal Data, Pindrop will provide reasonable assistance to Company in responding to data subject requests as required by Data Protection Laws. Unless required by applicable Law, Pindrop shall not respond to or take any action to comply with a data subject request without Company's approval.

****

Exhibit B - Implementation and Product-Specific Terms

1. Call Routing. The Product will be implemented and deployed based on an agreed to architecture for the routing of calls (the "**Approved Architecture**"). The Approved Architecture will apply for the duration of the applicable Subscription Term, unless Pindrop and Company mutually agrees otherwise in writing.

2. Pindrop Protect Cloud-Specific Terms.

(a) **Pindrop Database.** During the term of an Order, the Product will collect, process and analyze Company Call Data. Pindrop and its affiliates are authorized to use and contribute the Fraudulent Call Data to the Pindrop Database for the purpose of identifying, monitoring and tracking phone-based fraud and suspicious transactions or passively authenticating a caller for the purpose of identifying, monitoring and tracking phone-based fraud and suspicious transactions or passively authenticating a caller for the benefit of Company, Pindrop's and its affiliates' existing or future customers and the Consortium Members (the "**Authorized Use of Fraudster Data**"). Pindrop will only identify (i.e., "tag") that the Fraudulent Call Data was provided by Company on a pseudonymized basis (e.g., using a code name within the Pindrop Database itself). For clarity, neither Company nor any other customer of Pindrop has or will have access to or the ability to view the Pindrop Database or the data stored therein. Company agrees that the Authorized Use of Fraudster Data shall survive any termination or expiration of this Agreement and the applicable Orders.

(b) **Call Recording Storage Terms.** The following call recording storage and related terms shall apply to the configuration reflected in the applicable Order:

Company Storage of Company Call Recordings (default configuration unless specified otherwise in the applicable Order)

The default storage option for call recordings created by a Product in the ordinary course of its use is the use of Company's own Core Hosting Provider (as defined below) instance (i.e., under Company's own and direct account with the Core Hosting Provider (each a "**CHP Instance**"). For purposes of this Exhibit, "**Core Hosting Provider**" or "**CHP**" means the third party service provider whom Pindrop uses to host the Products covered under an Order (e.g., AWS or Google), as reflected in the applicable Order.

Company is solely responsible for all aspects of the CHP Instance, including without limitation, the cost of securing and maintaining the CHP Instances for the duration of the Orders as well as the security settings applicable to the CHP Instance.

The CHP Instance will be configured for use with a Product as set forth in the Approved Architecture, which configuration will include, at a minimum, (i) sufficient administrative and access rights for Pindrop to be able to monitor and maintain the call recordings as needed to deliver the Product as contemplated in the Documentation and for Pindrop to provide the maintenance and support for that Product (including sharing Company's share IAM credentials including access key, secret key and encryption settings with Pindrop until expiration of the applicable Subscription Term to enable such access); and (ii) the retention of the call recordings for the Calls as established from time to time based on Company's instructions and the standard features and functionality of the Product (collectively, the "**Minimum CHP Configuration Requirements**"). Company agrees to maintain the Minimum CHP Configuration Requirements for the CHP Instance for the duration of all Orders applicable to the Product, unless Company and Pindrop mutually agree otherwise in writing.

Upon the expiration or termination of Company's right to use a Product pursuant to one or more Orders, Company will be responsible for the deletion of any call recordings from the CHP Instance.

Pindrop Storage of Call Recordings

If the parties agree as part of the Approved Architecture that Pindrop, rather than Company, will store the call recordings created by the Product in its ordinary course of use on behalf of Company in Pindrop's CHP instance (i.e., under Pindrop's own and direct account with the CHP, such as AWS or Google) (each a "**Pindrop CHP Instance**"), then the following terms apply:

(i) Pindrop will maintain the call recordings based on the time period(s) configured within the Product as established from time to time based on Company's instructions and the standard features and functionality of such Product.

(ii) Company's Named Users will have access to the call recordings through the standard user interface for the Product to enable such Named Users to disposition a given Call as either fraudulent or genuine. No other administrative access will be granted to Company for the Pindrop CHP Instance.

(iii) Upon the expiration or termination of Company's right to use a Product pursuant to one or more Orders, then Pindrop will delete any remaining call recordings from the Calls from the Pindrop CHP Instance.

3. CHP Flow-Down Terms. In providing hosting and related cloud platform services ("**CHP Services**") to Company and notwithstanding anything to the contrary in the Agreement, Company acknowledges and agrees that (a) the CHP may require that Pindrop notify it of any unauthorized access and/or use by Company of the CHP Services and Company authorizes Pindrop to provide any such required notice to CHP; (b) Company's receipt of the CHP Services may be subject to legal intercept or monitoring activities by CHP, its suppliers or local authorities in accordance with its standard business practices and applicable Laws; and (c) Company may not use the CHP Services, or any interface(s) provided with the CHP Service, to access or use any other CHP product or service in a manner that violates the terms of service applicable to such other CHP product or service.

4. Managed Service Provider Terms. If Company is authorized pursuant to an Order to bundle a Product as part of Company's Managed Services (defined below), the incremental or different terms and conditions in this Section shall apply. To the extent of any conflict between this Section 4 and any other terms of this Agreement, the terms in this Section 4 shall control.

(a) **Definitions.**

(i) "Company Customer" has the meaning assigned in Section 11(c) (Procedural Requirements for Third Party Claims) of the main body of the Agreement.

(ii) "Company Customer Agreement" means a written agreement between Company and a Company Customers pursuant to which Company offers Products and Services as bundled with the Company Managed Services in connection with an Order.

(iii) "Company Managed Services" means a service whereby Company (a) assumes, performs or provides the one or more of the following (i) responsibility for day-to-day operations and management of all or a portion of Company Customer's call center data processing operations; or (ii) Company facility management, systems integration or similar services in connection with Company Customer's call center; or (iii) Company's business process outsourcing services in connection with Company's call center services; all regardless of whether the Product is located at the Company Customer's or a third party location or Company facility, and whether used on the Company Customer's or third party owned equipment, to the extent applicable, and (b) are accessing and using the Products and Services on behalf of or for the benefit of Company Customer.

(iv) "Managed Service Customer" means each of Company Customers who have entered into a Company Customer Agreement to obtain Company Managed Services from Company.

(b) **Bundled Offering.** Subject to terms and conditions of this Agreement and the Order(s), Pindrop grants to Company a non-exclusive, non-transferable, non-assignable right to bundle the Product solely as a non-severable part of Company Managed Services to Company Customers in the Authorized Geography. Company does not have the right to appoint or otherwise authorize any other third party, directly or indirectly, to perform any activities or exercise any rights granted to Company under this Agreement in connection with the Products and Services under this Agreement or any Order (whether as a sub-service provider or otherwise). Company will not make any false or misleading representations with regard to Pindrop, its affiliates, the Products or Services or any representations, warranties or guarantees with respect to the Products and/or Services that are inconsistent the terms of this Agreement or Documentation.

(c) **Company's Customer-Facing Requirements.** The Products and Services bundled by Company as part of Company Managed Service shall be made pursuant to the Company Customer Agreement, which shall be no less protective of the Pindrop Property than the applicable terms and conditions in this Agreement. As between Pindrop and Company, Company is solely and exclusively liable for all commitments and terms it agrees to in each Company Customer Agreement. Under no circumstances shall Pindrop be liable to each of Company Customers in connection with any Company Customer Agreement. As between Pindrop and Company, (i) Company is solely and exclusively responsible for providing appropriate notices and disclosures to each of the Company Customers with respect to Company Call Data and Outputs relative to the Calls applicable to each of the Company Customers and how such is collected, used, stored and the like (as detailed in this Agreement); and (ii) Company shall secure and maintain from each of the Company Customers the necessary rights for Company to grant Pindrop and its affiliates the rights and licenses under this Agreement and each Order, and enable Company to fulfil and comply with Company's obligations to Pindrop under this Agreement and each Order, including without limitation those terms and conditions applicable to the Company Call Data and Outputs.

(d) **Company's Service Provider Responsibilities.**

(i) **Customer-Unique Identifiers.** To enable differentiation of Calls, Company shall ensure that each Company Customer is assigned a unique identifier that is transmitted as part of the Company Call Data to the Product for each Call.

(ii) **Company Use of Behalf of Company Customers.** In Company's role as a service provider of Company Managed Services to Company Customers, Company is only permitted to use a Product solely to perform phone number fraud verification and/or authentication on behalf of and solely for each of Company Customers' own products or services based on the features and functionality enabled in the Product and for no other purpose (e.g., not for credit decisioning purposes or to determine a consumer's eligibility for credit or insurance, or for any other permissible purpose set forth in the FCRA). For avoidance of doubt, any use or purpose restrictions applicable to Company under this Agreement and any Order shall likewise apply to the Products and Company's bundling of such Products as part of the Company Managed Services.

(iii) **No Access or Use by Company Customers.** Company acknowledges and agrees that neither Company Customers nor any of Company Customers' personnel shall have access to or use of, either directly or indirectly, the Products or Services, including any Outputs. Company may, however, provide aggregated data with respect to the Calls analyzed by the Products to each Company Customer pursuant to written obligations of confidentiality with each Company Customer (i.e., quantity of calls analyzed, authenticated or for which fraud was detected, account status and the stand-alone risk score).

(iv) **Responsibility for Company Customers.** Any act or omission committed by a Company Customer that, if committed by Company (i.e., where Company has a responsibility pursuant to the terms and conditions of this Agreement or an Order) would be deemed a breach of this Agreement or the applicable Order will be considered a breach by Company, as applicable, including by way of example, a breach of the confidentiality obligations or a failure to comply with the obligations in 7 (Company Responsibility Statement) of the main body of this Agreement. Further, a breach by Company of the restrictions in the last sentence of Section 4(b) (Bundled Offering) above or Company's obligations under Section 4(c) (Company's Customer-Facing Requirements) above or any claim by a Company Customer that Company failed to comply with the Company Customer Agreement with Company Customer shall be (x) included within the scope of Company's obligations to Pindrop in Sections 11(b) (Company Coverage for Third Party Claims) and 11(c) (Procedural Requirements for Third Party Claims) of the main body of this Agreement; and (y) excluded from Company's limitations of liability for direct damages under Section 10(b) (Liability for Direct Damages) of the main body of this Agreement.

****

Exhibit C - Pindrop Information Security and BCP Programs

1. Definitions.

Capitalized terms used in this Exhibit C have the meanings given below or, if not defined below, the meanings given in the main body of this Agreement.

"Company Controlled System" means Information Systems that are within Company's possession or control.

"In-Scope Subcontractor" means each of Pindrop's subcontractors who are engaged by Pindrop to deliver component(s) of the Products or Services to Company and will have access to, process, or store Company Call Data.

"**Information System**" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

"**Pindrop-Controlled Systems**" means: (i) Information Systems that are within Pindrop's possession or control; and (ii) Amazon Web Services ("**AWS**") Information Systems or Google Cloud Platform ("**GCP**") that meet the following criteria: (a) under Pindrop's enterprise account with AWS or GCP, as applicable; (b) used by Pindrop to deliver the Products or Services or used by Pindrop for Pindrop's internal, corporate-level systems; and (c) are AWS Information Systems or GCP Information Systems for which Pindrop solely configures and manages the security controls used by Pindrop to protect the data stored within such AWS Information Systems or GCP Information Systems. For clarity, the defined term Pindrop-Controlled Systems excludes all Company Controlled Systems.

"Regulator" means any industry regulatory agency with supervisory authority over Company under applicable Laws.

"**Security Breach**" means a reasonably suspected or confirmed unauthorized disclosure of Company Confidential Information within Pindrop's possession or control; or a reasonably suspected or confirmed unauthorized access by a third party to any Pindrop-Controlled Systems that process, hold, or provide access to Company Confidential Information.

2. Governance and Oversight.

(a) Pindrop will have in place a cybersecurity program designed to protect the confidentiality, integrity, and availability of the Pindrop-Controlled Systems, as detailed in this Exhibit C. Such cybersecurity program includes tracking data asset locations and maintaining a risk based written security policy or policies that satisfy the requirements set forth in this Exhibit C (the "**Security Policy**"). Pindrop will not make any change to its Security Policy that will materially degrade the overall level of security described in this Exhibit C.

(b) The Security Policy will be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Company's Confidential Information within Pindrop's possession or control that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. The risk assessment will be written and include: (i) criteria for the evaluation and categorization of identified security risks or threats to Company's Confidential Information within Pindrop's possession or control; (ii) criteria for the assessment of the confidentiality, integrity, and availability of Company's Confidential Information within Pindrop's possession or control, including the adequacy of the existing controls in the context of the identified risks or threats; and (iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Security Policy will address the risks.

(c) Pindrop will periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Company's Confidential Information within Pindrop's possession or control that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

(d) Pindrop will (i) design and implement safeguards to control the risks identified through the risk assessments it performs; and (ii) evaluate and adjust its information security program in light of the results of the testing and monitoring described in this Exhibit C, any material changes to Pindrop's operations or business arrangements, and any other circumstances that Pindrop knows or has reason to know may have a material impact on Pindrop's information security program.

(e) Pindrop will assign an appropriate individual within Pindrop's Information Security team to maintain responsibility and executive oversight for the Security Policy, including, without limitation, implementation, formal governance and revision management, employee education, and compliance enforcement. The individual assigned by Pindrop to maintain responsibility and

executive oversight for the Security Policy will report in writing, regularly and at least annually, to Pindrop's executive team, board of directors or equivalent governing body. Any such reports will include the following information: (i) the overall status of Pindrop's information security program; and (ii) material matters related to Pindrop's information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, compliance obligations and recommendations for changes in the information security program.

(f) Subject to the terms and conditions in Section 13 (Audits) of the main body of the Agreement, the rights in this Section 2(f) shall apply. If a Regulator exercising its supervisory authority makes a request to Company to access the Products or Services, Company will use commercially reasonable efforts to resolve that request directly with the Regulator using alternative methods, including by reviewing the security certifications for the Pindrop-Controlled Systems with the Regulator. If the Regulator determines that the information available through these mechanisms is insufficient to verify compliance with applicable Laws then, upon the Regulator's request and Company's written confirmation that the Regulator has the requisite supervisory authority over Company to make such a request, Pindrop will provide the Regulator with: (i) information about the Products and Services and the opportunity to discuss the Products and Services operations and controls with Pindrop subject matter experts; and (ii) if required, a direct right to examine the Products and Services used by Company, including by conducting an examination on premises. Pindrop may charge Company a fee (based on Pindrop's reasonable costs) for any such discussion, communication, and examination. Any discussion, communication, or examination requested by the Regulator under this subsection will, except in an emergency or crisis situation, be conducted consistent with the terms of Section 13 (Audits) of the main body of the Agreement.

3. Policies and Procedures.

(a) The policies that comprise the Security Policy are commercially reasonable, communicated to relevant Pindrop employees, and designed to: (i) be protective of Company's Confidential Information within the Pindrop-Controlled Systems; and (ii) support Pindrop's compliance with its obligations under the Agreement. If requested by Company in writing, Pindrop agrees to provide Company with (1) the title page and table of contents related to the Security Policy or other related policies or procedures applicable to Pindrop's business operations set forth in this Exhibit C; (2) an opportunity to discuss Pindrop's security measures; (3) confirmation that penetration testing and vulnerability scanning has been performed; and (4) independent audit reports applicable to the Products (such as SOC2 Type 2) that Pindrop makes generally available to its customers under confidentiality terms.

(b) Pindrop will review the Security Policy at least annually and amend the Security Policy (or subparts thereof) as Pindrop deems commercially reasonable (e.g., in light of relevant risk assessment findings, relevant changes in applicable laws or standards, technology advances, changes to Pindrop's systems or Pindrop's own changing business operations).

(c) As part of the Security Policy, Pindrop will have security-minded development practices for applications that form any part of the Products or that are used to deliver the Products, and procedures for evaluating and assessing the security of externally developed applications that form any part of the Products or that are used in the delivery of the Products.

(d) Pindrop will maintain and follow employment verification requirements for all new Pindrop employee hires, with such verifications occurring prior to the date of hire. These requirements will include criminal background checks, proof of identity validation, and additional checks as deemed reasonably necessary by Pindrop and as permitted by applicable Law. Such employment verification measures shall be in line with requirements under Industry Standards (as defined in Section 4 (Compliance) below). Each Pindrop local entity is responsible for implementing the foregoing requirements in its hiring process as applicable and permitted under local law. Pindrop will provide verification of the completion of background checks for employees upon Company's reasonable request; however, Pindrop is not required to provide an actual copy of the background check results.

(e) Pindrop will have a training program that includes conducting security education for its employees annually. The training program will: (i) provide security awareness training that is updated to reflect risks identified by Pindrop's risk assessments; and (ii) promote the maintenance of current knowledge of changing information security threats and countermeasures.

4. Compliance. Pindrop-Controlled Systems will be subject to annual certification of compliance with the Payment Card Industry Data Security Standards (PCI-DSS) (with respect to relevant cardholder data environments only), ISO 27001, and SSAE SOC 2 or any substantially equivalent or alternative successor standard (the "**Industry Standards**"). Upon written request from Company, Pindrop will provide evidence of the compliance and accreditation with the Industry Standards as reasonably determined by Pindrop, such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard). Additionally, Pindrop will use commercially reasonable efforts to verify that its In-Scope Subcontractors comply with all Laws applicable to the operation of the In-Scope Subcontractors' business and all Laws generally applicable to providers of information technology services, in each case, to the extent relevant to the specific products and services being provided by such In-Scope Subcontractor to Pindrop in connection

with the Products and Services covered under the Agreement and an Order. The verification may be accomplished through Pindrop's vendor due diligence process. If Pindrop's vendor due diligence process identifies a non-compliance with the aforementioned Laws, Pindrop will work with the In-Scope Subcontractor to cure such deficiency.

5. Incident Response and Security Breaches.

(a) Pindrop will maintain and follow documented incident response policies consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines or equivalent industry standards for computer security incident handling. Pindrop's written incident response plan will be designed to promptly respond to, and recover from, any event materially affecting the confidentiality, integrity, or availability of Company's Confidential Information within Pindrop's possession or control. Such incident response plan shall address the following areas: (i) the goals of the incident response plan; (ii) the internal processes for responding; (iii) the definition of clear roles, responsibilities and levels of decision-making authority; (iv) external and internal communications and information sharing; (v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (vi) documentation and reporting; and (vii) the evaluation and revision as necessary of the incident response plan.

(b) Pindrop will investigate Security Breaches (and security incidents that are not yet Security Breaches but that are reasonably likely to result in Security Breaches) of which Pindrop becomes aware, perform a root-cause analysis of the same and take prompt action designed to contain the Security Breach. Company must notify Pindrop of any suspected vulnerability or security incident by immediately submitting a technical support request to Pindrop.

(c) Pindrop will notify Company within no more than 24 hours after Pindrop becomes aware of a Security Breach that has impacted Company's Confidential Information. Pindrop will provide Company with reasonably requested information about such Security Breach and the status of any Pindrop containment and service restoration activities.

6. Physical Security and Entry Control.

(a) Pindrop will maintain reasonable physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, designed to protect against unauthorized entry into Pindrop-managed facilities (i.e., its headquarters) used to provide the Pindrop-Controlled Systems. Auxiliary entry points into such facilities, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

(b) Access to Pindrop-managed facilities and controlled areas within those facilities will be limited by job role and subject to authorized approval. Such access will be logged, and such logs will be retained for not less than one year. Pindrop will revoke access to Pindrop-managed facilities upon separation of an authorized employee. Pindrop will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

(c) Any person granted temporary permission to enter an Pindrop-managed facility or a controlled area within such facility will be registered upon entering the premises and will be escorted by authorized personnel.

(d) Pindrop will take precautions designed to protect the physical infrastructure of Pindrop-managed facilities against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

7. Access, Intervention, Transfer and Separation Control.

(a) Pindrop will maintain measures for Pindrop-Controlled Systems that are designed to logically separate and prevent Company's Confidential Information stored within Pindrop-Controlled Systems from being exposed to or accessed by unauthorized persons. Pindrop will maintain isolation of its production and non-production environments, and, if Company's Confidential Information is transferred to a non-production environment, for example to reproduce an error at Company's request, security and privacy protections in the non-production environment will be equivalent to those in production.

(b) Pindrop will encrypt Company's Confidential Information that is subject to long-term storage within Pindrop-Controlled Systems and when Company's Confidential Information is transmitted by Pindrop over public networks. Pindrop will maintain documented procedures for encryption key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use. To the extent that encryption is impractical, Pindrop will use compensating controls designed to protect Company's Confidential Information.

(c) If Pindrop requires access to Company's Confidential Information that is stored within Pindrop-Controlled Systems, and if such access is managed by Pindrop, Pindrop will deploy measures designed to restrict access to the minimum level required. Such access, including, without limitation, administrative access, will be individual, role-based, and subject to approval and regular

validation by authorized Pindrop personnel following the principles of segregation of duties. Pindrop will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or upon the request of authorized Pindrop personnel, such as the account owner's manager.

(d) For Pindrop-Controlled Systems, Pindrop will:

(i) monitor and periodically test the Pindrop-Controlled Systems to assess the effectiveness of the Security Policy;

(ii) maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and password change frequency;

(iii) monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access and activity; (2) facilitate a timely and appropriate response, and (3) enable internal and independent third-party audits of compliance with the Security Policy;

(iv) where practicable for a given Pindrop-Controlled System, use multi-factor authentication designed to protect against unauthorized access to such Pindrop-Controlled System;

(v) maintain logs in which privileged access and activity are recorded will be retained in compliance with Pindrop's worldwide records management plan and Security Policy;

(vi) maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of the logs described in the prior (v);

(vii) maintain tools designed to detect and remove Malicious Code from the Pindrop-Controlled Systems;

(viii) adopt procedures for change management; and

(ix) develop, implement, and maintain procedures for the secure disposal of Company's Confidential Information within Pindrop's possession or control in any format used in connection with the provision of the Product or Service to Company to which it relates, unless such information is necessary for business operations or for other legitimate business purposes or as otherwise expressly authorized by Company in this Agreement or an Order, is otherwise required to be retained by law or regulation, as set forth in Section 11(e) (Obligations Upon Termination) in the main body of this Agreement, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

(e) Pindrop will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitization. Upon Company's reasonable request, Pindrop will provide a certificate of destruction certifying the destruction of any of Company's Confidential Information within Pindrop's possession or control.

8. Service Integrity and Availability Control. With respect to Pindrop-Controlled Systems, Pindrop will:

(a) Perform security risk assessments at least annually;

(b) Perform security testing and vulnerability assessments on a periodic basis;

(c) Enlist a qualified testing service to perform penetration testing at least annually;

(d) Perform automated vulnerability scanning against configuration industry standards reasonably designed to identify publicly-known security vulnerabilities in Pindrop-Controlled Systems based on Pindrop's risk assessment: (i) at least every six months; (ii) whenever there are material changes to Pindrop's technical operations of the nature that reasonably justify the performance of a scan; and (iii) whenever there are circumstances that Pindrop knows or has reason to know may have a material impact on Pindrop's information security program of the nature that reasonably justify the performance of a scan;

(e) Follow Pindrop's policies with respect to the remediation of identified vulnerabilities, based on associated risk, exploitability, and impact;

(f) Take reasonable steps to avoid disruption of the Products and Services when performing its tests, assessments, scans, and execution of remediation activities;

(g) Maintain measures designed to assess, test, and apply security advisory patches. Upon determining that a security advisory patch is applicable and appropriate, Pindrop will implement the patch pursuant to Pindrop's policies, taking into account associated risk, exploitability, and impact;

(h) Maintain policies and procedures designed to manage risks associated with the application of changes; and

(i) Maintain an inventory of information technology assets.

9. Malicious Code. Pindrop will not intentionally or knowingly either introduce or allow the introduction of any code, files, scripts, agents or programs intended to do harm, including for example, viruses, worms or Trojan horses ("**Malicious Code**") into the Product delivery environment. If Malicious Code is found to have been introduced into a Product by Pindrop, Pindrop will be responsible for removing the Malicious Code from such Product. If the Malicious Code that was found to have been introduced by Pindrop is also found to have been introduced into Company Controlled Systems, Pindrop will reasonably cooperate with Company by providing relevant information necessary for the Company to mitigate the effects of such Malicious Code.

10. Vendor Management Program.

(a) Pindrop agrees to maintain a formal vendor management program. As part of such program, Pindrop is responsible for conducting due diligence on each of its In-Scope Subcontractors on a periodic basis to assess the extent to which each In-Scope Subcontractor has reasonable security measures designed to protect Company Call Data in that In-Scope Subcontractor's possession or control. In conducting In-Scope Subcontractor due diligence, Pindrop may rely upon the information available in an In-Scope Subcontractor's SOC2 or comparable report or certification (each an "**Independent Audit Report**") to make such assessment, even if the Independent Audit Report does not contain the level of detail specified in this Exhibit C. Upon Company's request, Pindrop shall direct Company to the location at which Company can obtain copies of an In-Scope Subcontractor's Independent Audit Report. If Company is unable to obtain such Independent Audit Report, Pindrop shall use reasonable efforts to secure the relevant Independent Audit Report from such In-Scope Subcontractor and provide a copy to Company. Pindrop agrees to provide Company with a minimum of 30 days' prior notice if there is a material change in the identity of the In-Scope Subcontractors applicable to the Products or Services covered under an existing Order. If an In-Scope Subcontractor is Processing Company Personal Information, then within 30 days of receiving notice of a new In-Scope Subcontractor, Company may object (in good faith) to such engagement. In the event Company makes an objection within such time period, the parties will work in good faith to resolve the objection. If the parties are not able to come to a mutually agreed to solution, Company's sole and exclusive remedy will be to terminate the relevant Order under which the new In-Scope Subcontractor is Processing Company Personal Information pursuant to the terms in the Marketplace Agreement and such Order(s).

(b) In addition to In-Scope Subcontractors, Company understands and agrees that Pindrop may use other vendor systems and solutions to support its day to day back office business operations where Company Confidential Information (other than data that's been input into a Product) may be collected, processed or stored, including by way of example, contract management, billing or other financial transaction-related tools and solutions (each a "**Back Office Business System**"). Back Office Business Systems are not Pindrop-Controlled Systems, but are subject to the requirements in Sections 10(c) and 10(d) of this Exhibit C.

(c) Pindrop will have a written agreement in place with each In-Scope Subcontractor and each vendor providing a Back Office Business System that contains commercially reasonable confidentiality obligations designed to protect the confidentiality of Company Call Data in the possession or control of the In-Scope Subcontractor or the confidentiality of Company's Confidential Information in the possession or control of each vendor providing the Back Office Business System, as applicable.

(d) Pindrop is responsible for any unauthorized disclosure of Company Call Data by an In-Scope Subcontractor and Company's Confidential Information by each vendor providing a Back Office Business System to the same extent as Pindrop itself would be by the terms of this Agreement.

11. BCP Program.

(a) Pindrop's BCP will include (i) a business impact analysis that includes a risk assessment that documents prioritization of business functions and process, systems, subcontractors, resource requirements and interdependencies that may affect recovery timelines and alternative resource plans; (ii) specifically defined or targeted RTOs (recovery time objective); and (iii) specifically defined or targeted RPOs (recovery point objective). Unless provided otherwise in an Order, Pindrop's RTO and RPO policy for a single availability zone failure for a Product will not exceed 24 hours.

(b) Pindrop will conduct periodic exercises with respect to its BCP (such as tabletop exercises), but on no less than an annual basis. If an event triggers Pindrop's BCP (each a "**BCP Event Trigger**"), Pindrop is responsible for implementing the BCP in accordance with Pindrop's policies and procedures. Company understands and agrees that if a BCP Event Trigger occurs, depending on the nature and scope of the event and whether Company procures "high availability" Appliances for any Products deployed at Company's managed facilities, the availability and/or ability to recover Company's Confidential Information, including without limitation, the Company Call Data, in Pindrop's possession or control may be impacted.

(c) The Products are not designed for and should not be used by Company as an official record or similar, whether for regulatory purposes or otherwise.

(d) Should the Product(s) in use by Company experience an outage, Pindrop will notify Company of such outage and provide periodic status updates until such impact is resolved.

(e) Pindrop will provide reasonable prior notice to Company if Pindrop's BCP is changed in a way that would have a material adverse impact in Pindrop's ability to deliver the Products or the Services to Company as set forth in the Agreement and each Order.

12. Company's Responsibilities. Company agrees to take commercially reasonable measures designed to detect and prevent the introduction of Malicious Code into Pindrop-Controlled Systems used in the delivery of Products or Services to Company. Company further understands and agrees that Company is responsible for determining whether the Products and Services are suitable for Company's use and implementing and managing security measures for all components of the Products and Services that Pindrop does not manage or for which Pindrop does not have security obligations under this Exhibit C, with Pindrop's only security obligations being as set forth in this Exhibit C. Examples of Company's responsibilities include, without limitation: (a) securing all of Company Controlled Systems; and (b) accepting and implementing all security patches provided by Pindrop with respect to any On-Premises Appliances (and all other software distributed by Pindrop to Company in order to enable such security patches), without delay. Company further agrees that it is Company's responsibility, and not Pindrop's responsibility, to ensure adequate backups of any of Company Call Data on Company Controlled Systems that are physically and logically separated from the Products and Services being provided by Pindrop under this Agreement. Company agrees that Pindrop shall not be in breach of its obligations under this Exhibit C if and to the extent that Pindrop's non-compliance is directly caused by Company's failure to comply with Company's own security responsibilities in this Agreement.

****

Exhibit D - AI Terms

1. Company's Access to Pindrop's Model Documentation. Upon request, Pindrop shall reasonably cooperate with Company to provide reasonable information or documentation about the AI Tools in use by the Products such as (1) a reasonable description of such AI Tools, use in the Products, the purpose for which they are used, and their intended output, results, or outcomes; and (2) a reasonable description of the processes and procedures Pindrop uses to develop, implement and use the AI Tools within the Products and their output to validate that the AI Tools are reasonably performing reliably for their intended use such as Pindrop's standard model development documentation it makes available to its customers, a current copy of which will be promptly provided to Company on Company's written request. Notwithstanding the foregoing, Pindrop shall not be required to share any trade secrets or any data or information about its AI Tools that Pindrop believes in its good faith business judgment represents sensitive information about the AI Tools or how they operate in practice, including by way of example only, the specific input features (direct or derived) or the weighting of risk factors. For clarity, the foregoing does not include general categories of inputs or the actual results from the weighting with respect to the Models.

2. When Company Prior Approval Is Required. Unless pre-approved by Company in writing (including as stated in an applicable Order), the following apply:

(a) The Products do not have or use any generative AI functionality (whether proprietary or publicly available), nor do they use any large language learning models (LLMs) (each "**Non-Approved AI**") to process Company Call Data with the Products covered under this Agreement. Pindrop will not use or otherwise deploy any Non-Approved AI in the Product without Company's prior written approval.

(b) Pindrop will not use the "voice features" extracted by the Product from Company's Calls to train Pindrop's AI Tools or benefit customers other than Company.

(c) Pindrop warrants that the AI Tools in the Product were developed by Pindrop, deployed by Pindrop, and are used and maintained by Pindrop in a way that treats impacted individuals free of unlawful bias or discrimination and will not adversely impact the rights or safety of individuals when used by Company in accordance with the applicable Documentation for the Product, the terms and conditions of this Agreement and in compliance with applicable Laws. As between Pindrop and Company, Company is solely responsible for the actions Company takes using the Outputs, and Company controls where and how the Outputs for Company's business purposes based on Company's own policies and procedures.

3. Conditions for Approval of AI Tool Use.

(a) Pindrop acknowledges that Company's approval and use of the AI Tools in the Products are limited to the AI Tools as outlined in this Agreement or Company's other written approval, including in an Order.

(b) Pindrop is responsible for monitoring the quality and performance of the AI Tools in the Products and for taking reasonable steps to address significant deteriorations in the AI Tool's performance in a Product in use by Company, as measured by the metrics captured in Pindrop's then-current model monitoring plan applicable to Company's current use and configuration of each Product. Company understands that minor fluctuations that are normal for any models are not considered a "deterioration" of the AI Tool's performance for purposes of this Section.

For the purposes of this Agreement, the following definitions apply:

"**AI Tool(s)**" means a system, application, algorithm, statistical model or other technology that can perform tasks that typically require human intelligence, including understanding natural language, recognizing patterns, solving problems, making predictions, interpreting and processing data or that are prompted by inputs it receives to produce outputs, such as predictions, classifications, prescribed actions, content, recommendations or decisions. AI Tools include machine learning-based algorithms for fraud risk, authentication and audio and video manipulation technologies (e.g., voice cloning, deepfakes). For purposes of clarity, AI Tools include Models.

“**Model(s)**” (Machine Learning Model) means a mathematical representation that, once trained on a dataset, can be used to make predictions and classifications on new data by learning patterns, in each case, to produce outputs from a given set of inputs within or incorporated into a Product.