Master Services Agreement

This Master Service Agreement ("Agreement") shall apply to the sale of Services from Convercent, Inc. ("Convercent") to its customer ("Customer"), unless Convercent and Customer enter into or have entered into another agreement regarding the Services contemplated herein, and such agreement is in effect as of the Effective Date ("Existing Agreement"), in which case the terms and conditions of the Existing Agreement shall govern the sale of those Convercent Services. Absent an Existing Agreement, this Agreement is effective as of the date an Order Form or Purchase Order is executed ("Effective Date").

1. Services.

1.1 Order Forms. During the Term, and subject to the terms and conditions of this Agreement and Customer's payment of all applicable Fees, Convercent will provide to Customer the Services identified in one or more Order Forms executed by both parties (each, an "Order Form"). Order Forms are incorporated by reference into this Agreement. To the extent of any conflict between this Agreement and an Order Form, the Agreement shall control, except to the extent the Order Form expressly identifies a provision of the Agreement to be superseded by the Order Form. The "Services" shall consist of the products and modules provided via a Convercent website and/or mobile application, all user documentation, information and materials contained within such products or modules, and related support, professional services and other services provided by Convercent as explicitly identified in one or more Order Forms. Customer shall not use the Services beyond the limitations set forth in an Order Form.

1.2 Use of the Services. Customer may use the Services ordered by Customer solely for Customer's internal business purposes. Customer may store up to fifty (50) gigabytes of Customer Data on the Services and utilize bandwidth up to one (1) terabyte. Customer is solely responsible for (a) all actions or omissions of Customer or its authorized Services users in connection with the Services, whether or not authorized by Customer; (b) configuring the Services for Customer's use; (c) granting authority for use of the Service within Customer's organization, and providing user name and password access instructions securely through the Service; (d) providing for and maintaining any systems, software, hardware, web browser and Internet service necessary to access and use the Services, including current versions of web browser programs supported by Convercent; and (e) establishing, managing, maintaining, and supporting access rules, incident reporting protocols, authorization of Customer representatives to receive incident reports and communications and any other distribution rules regarding the Services or information contained therein.

1.3 Restrictions. Customer and its employees or representatives shall not (a) modify, make derivative works of, reverse engineer, disassemble, decompile, or otherwise attempt to discover the source code for the Services; (b) copy, distribute, encumber, sell, rent, lease, sublicense, loan, or otherwise transfer rights to the Services, or otherwise permit any third party to use the Services or use the Services on behalf of or for the benefit of any third party; (c) use, evaluate or view the Services for the purpose of designing, modifying, or otherwise creating any environment, program, or infrastructure or any portion thereof, which performs functions similar to the functions performed by the Services; or (d) remove or alter any trademark, logo, copyright, or other proprietary notices, legends, symbols, or labels in the Services.

1.4 Additions to the Services. Convercent may from time to time in its discretion make available to its customers one or more optional products, modules or features for the Services, which require additional one-time or recurring fees and may be subject to additional terms and conditions. The Services as defined herein shall include only those additional products, modules or features that are ordered by Customer pursuant to an Order Form. Customer will be under no obligation to subscribe to such optional products, modules or features. Customer may submit written incident reports online through the Services in English or in another supported language indicated within the Services. Translation of written incident reports and other documents submitted in languages not then supported by Convercent shall be subject to additional fees.

1.5 Service Levels.

1. *Web Application*. Convercent will maintain 99.8% uptime of the web based Services (the "Web Application SLA"). The calculation of uptime will exclude scheduled downtime and events not reasonably expected to be under the control of Convercent. Convercent will inform Customer reasonably in advance of any scheduled downtime.

2. *Call Center*. To the extent applicable to Services ordered by Customer pursuant to an Order Form, the call center shall be available to receive telephonic reports in the event of an outage within the web application and 80% of Customer's calls to the call center shall be answered in 20 seconds or less (the "Call Center SLA", which, along with the Web Application SLA is referred to as the "SLA"). To receive this SLA, Customer's Order Form must include dedicated phone lines.

3. *Remedy*. Convercent's sole liability (and Customer's exclusive remedy) for Convercent's breach of either or both SLAs shall be to issue a service credit ("Service Credit") for the applicable Services for the applicable month, in the amount specified in the table below. Such Service Credit shall be issued within thirty (30) days of written request by Customer. In the event two SLA remedies apply, Convercent will provide a service credit for the higher amount.

Actual Web Application Service Level for the month (% of uptime)	Actual Call Center Service Level for the month (% of calls answered in 20 seconds or less)	Service Credit to be issued (% of Customer service fees)
99.0 - 99.79%	75.0 – 79.99%	5%
98.0 – 98.99%	70.0 – 74.99%	10%
95.0 – 97.99%	65.0 – 69.99%	25%
90.0 – 94.99%	60.0 – 64.99%	50%
less than 90%	Less than 60%	100%

2. Intellectual Property Ownership and Licenses.

2.1 The Services. The Services and all components thereof are licensed, not sold. Convercent and its suppliers exclusively own and retain all rights, title, and interest in and to the Services (including software, user interface designs, and documentation) and all additions and modifications to the Services, including all intellectual property rights therein. Subject to the terms and conditions of this Agreement, during the term, Convercent will provide, to or on behalf of Customer, the Services components specified in the applicable Order Form, provided that, with respect to provision of all subscription-fee-based Services, the Customer Number does not increase compared to the Customer Number (a) specified in the applicable Order Form or (b) subsequently agreed to by the parties as the applicable Customer Number. "Customer Number" means the total number of employees and contract employees of Customer and all its affiliates. Customer represents the initial Customer Number specified on each Order Form is accurate. Convercent may request and Customer shall provide the then-current Customer Number from Customer prior to each anniversary of the Effective Date.

2.2 Customer Data. "Customer Data" means all data, information, reports, policies, and other content imported to the Services or otherwise provided to Convercent or its contractors by or for Customer in connection with Customer's use of the Services, and all data and information received by or for Customer from Customer's use of the Services. "Customer Data" includes all "Personal Data" as defined in below and all "Restricted Data" as defined in Exhibit A. Customer exclusively owns and retains all rights, title and interest in and to the Customer Data, except for pre-existing Services components contained in such Customer Data (e.g., incident report templates). Customer hereby grants to Convercent and its authorized representatives and contractors a non-exclusive and non-transferable right and license to use, process, store, and transmit, and disclose Customer Data solely to provide the Services to Customer and fulfill other obligations described in this Agreement. Customer further authorizes Convercent to aggregate Customer Data with similar data from other Convercent customers in a manner that does not identify Customer or include any Personal Information (defined below), to further develop the Services for Convercent customers.

3. Customer Participation in Joint Marketing Activities.

3.1 Use of Name and Logo. During the Term, Convercent may include Customer's name and logo as a customer who uses the Services, in Convercent's standard marketing materials in which it references other customers.

3.2 Following implementation of the software Services, at a time mutually agreeable to the parties, Customer will participate in the following joint marketing activities:

1. Customer's Chief Compliance Officer or a comparable senior executive ("Executive") will participate in periodic Convercent marketing events and webinars as a guest speaker;

2. Executive will take periodic calls from reporters, other members of the press, and industry analysts;

3. Executive will take periodic reference calls from other Convercent sales prospects;

4. Executive will conduct a video interview regarding why Customer chose Convercent; and

5. Customer will issue a joint press release with Convercent.

4. Fees and Taxes.

4.1 Customer agrees to pay the fees set forth in each Order Form ("Fees") in U.S. dollars. Customer may not offset any amounts due to Convercent hereunder against amounts due to Customer. Fees not paid on or before the applicable due date will accrue a late fee at a rate of 1.5% per month (or the maximum rate permitted by law). Customer shall be liable to Convercent for attorneys' fees and all other reasonable costs associated with collecting such Fees.

4.2 As indicated in the Order Form, Convercent's fees do not include any taxes, levies, duties or similar governmental assessments of any nature (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder, excluding taxes on Convercent's net income. If Convercent has the legal obligation to pay or collect Taxes for which Customer is responsible under this, Convercent will invoice Customer and Customer will pay that amount unless Customer provides Convercent a valid tax exemption certificate from the appropriate taxing authority.

5. Term and Termination.

5.1 Term. This Agreement will commence on the date the Order Form is executed or Purchase Order referencing the Order Form is received (the "Effective Date") and, unless earlier terminated in accordance with Paragraph 4.2, shall remain in effect so long as any Order Form remains in effect (collectively, the "Term").

5.2 Termination. Either party may terminate an Order Form upon written notice if the other party is in material breach of this Agreement or Order Form and such breach remains uncured for thirty (30) days following the breaching party's receipt of written notice of such breach.

5.3 Effect of Termination. Upon expiration or termination of this Agreement for any reason: (a) the rights and licenses granted hereunder shall cease and the Services will immediately terminate, (b) if requested by Customer, Convercent will make available to Customer (via an SFTP site, for example) the Customer Data held by Convercent (and Customer will assume responsibility for its copy of such Customer Data (and any access thereto) upon download of the Customer Data), (c) if requested by Customer, Convercent will take reasonable steps to assist with transfer of any dedicated phone numbers used by Convercent or its contractors in connection with the Service and (d) no less than once per year, following where applicable subsection (b) of this Paragraph 4.3, Customer Data shall be deleted from the application and any Customer Data residing on cloud-based back-ups shall be overwritten in accordance with Convercent procedures. Upon termination by Convercent for Customer's breach, prepaid fees shall not be refunded, and any overdue Fees shall be immediately due and payable. Upon termination by Customer for Convercent's breach, prepaid Fees for Services applicable to the period following termination shall be refunded to Customer, and any overdue Fees for Services provided up to the date of termination shall be immediately due and payable. Termination of the Agreement shall be without prejudice to either party's rights to seek recovery of damages or pursue any other remedies it may have hereunder or under applicable law. Paragraphs 1.3, 2, 4, 5.3, and 6 through 12 shall survive the Term and termination of this Agreement for any reason.

6. Confidentiality. Each party (the "Receiving Party") acknowledges that the Confidential Information (as hereinafter defined) of the other party (the "Disclosing Party") may contain information valuable to the Disclosing Party, and each Receiving Party agrees that Confidential Information shall remain the property of the Disclosing Party. Receiving Party shall not make use of Disclosing Party's Confidential Information, except as authorized by this Agreement and to the extent necessary for performance or enforcement of this Agreement; and Receiving Party shall keep Disclosing Party's Confidential Information confidential and not disclose to any third party, except to such Receiving Party's employees and contractors who need to know such information in order for such party to perform this Agreement and only to the extent they are bound by confidentiality and non-use obligations not less restrictive than this Agreement. If Customer provides any feedback, comments, or ideas to Convercent regarding the Services or improvements thereto, Customer agrees that Convercent will be free to use, disclose, and exercise any rights in the same in connection with its products and services. "Confidential Information" means all information that is, or should be reasonably understood to be, confidential or proprietary information of the Disclosing Party (and its suppliers, contractors and customers), including without limitation information concerning its business, products, services, finances, employees, contractors, software, notes, documentation, tools, processes, protocols, product designs and plans, customer lists and other marketing and technical information; and the terms of this Agreement, whether disclosed orally or in writing by any other media. "Confidential Information" includes all software and related user documentation included in the Services, Customer Data, and excludes information that (a) is or becomes generally known to the public through no fault or breach of this Agreement by the Receiving Party; (b) is independently developed by a party without reference to the Confidential Information of the other party; (c) was in the Receiving Party's possession free of any obligation of confidence at the time it was communicated to the Receiving Party; or (d) is rightfully obtained by a party from a third party without restriction on use or disclosure. Notwithstanding the foregoing, the Receiving Party shall not be in violation of this Paragraph with regard to a disclosure of Confidential Information (including Customer Data) that was in response to an order or subpoena of a court, agency or tribunal of competent jurisdiction, or pursuant to any applicable law or regulation, provided that the Receiving Party provides the Disclosing Party with prior written notice of such disclosure to the extent reasonably practicable and legally permissible in order to permit the Disclosing Party to seek confidential treatment of such information.

7. Representations and Warranties; Disclaimer. Each party represents and warrants to the other party that (a) it has and shall have full right and authority to enter into this Agreement and to grant the rights provided hereunder, (b) this Agreement shall be enforceable against it, and (c) the entry into and performance of this Agreement by it do not contravene other agreements, laws, or orders to which it is subject. CONVERCENT DOES NOT MAKE, AND TO THE FULLEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW, CONVERCENT EXPRESSLY DISCLAIMS, AND CUSTOMER HEREBY WAIVES, ALL REPRESENTATIONS, WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, REGARDING THE SERVICES OR CUSTOMER'S RESULTS FROM USING THE SERVICES, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF PERFORMANCE, NON-INFRINGEMENT, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR ANY EXPRESS OR IMPLIED

WARRANTIES OR CONTRACT TERMS OR AMENDMENTS ARISING OUT OF COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE. WITHOUT LIMITING THE FOREGOING, CONVERCENT DOES NOT REPRESENT OR WARRANT THAT THE SERVICES WILL MEET ALL OF CUSTOMER'S REQUIREMENTS OR BE UNINTERRUPTED, SECURE, COMPLETE, ERROR-FREE, OR FREE OF VIRUSES, MALICIOUS CODE, OR OTHER HARMFUL COMPONENTS, OR THAT ALL DEFECTS WILL BE CORRECTED.

8. **Indemnification**.

8.1 **By Convercent**. Convercent shall defend Customer and its employees, officers, directors, shareholders, partners, members, owners, agents, predecessors, and permitted successors and assigns from and against any third-party claim, demand, suit, action or proceeding ("Claim") which alleges that the Services infringe, misappropriate or violate the intellectual property right of any third party, or violate any applicable law or regulation. Convercent will pay all costs of defense and all damages finally awarded or paid in settlement of any such Claim.

8.2 **By Customer**. Customer shall defend Convercent and its employees, officers, directors, shareholders, contractors, partners, members, owners, agents, predecessors, and permitted successors and assigns from and against any and all Claims which allege that any Customer Data infringes, misappropriates or violates the intellectual property right or other right of any third party; allege any violation of applicable law by Customer in connection with its use of the Services; or which relate to or are based on any event, claim or matter that is reported to Customer via the Services. Customer shall pay all costs of defense and all damages finally awarded or paid in settlement of any such Claim.

8.3 **Indemnification Procedure**. Each party's indemnification obligation above is subject in each instance to the indemnified party (i) promptly giving notice of the claim to the indemnifying party; (ii) giving the indemnifying party sole control of the defense and settlement of the claim (provided that the indemnified party shall have the right to approve any material liability imposed on and borne by the indemnified party in connection with such settlement); and (iii) providing to the indemnifying party all available information and reasonable assistance. The remedies described above shall be the sole and exclusive remedy of the indemnified party and the sole obligation of the indemnifying party for third party Claims.

8.4 **Exceptions**. Notwithstanding the foregoing, Convercent shall not have any indemnification obligations pursuant to this Agreement to the extent any Claim arises from (i) use of the Services outside the scope of the rights granted to Customer in this Agreement; (ii) use of the Services with other products, software or materials not furnished by Convercent where the Services would not themselves be infringing; or (iii) the modification or improvement of the Services by Customer or any third party; or (iv) any continued use by Customer of an allegedly infringing item or continued allegedly infringing activity by Customer after Convercent has replaced or modified the item or instructed Customer to modify the activity so that it becomes non-infringing.

8.5 **Replacement or Modification**. Should the use of any Services or portion thereof be enjoined or threatened to be enjoined or determined to be infringing any third party intellectual property right, Convercent will notify Customer and, at Convercent's expense: (a) procure for Customer the right to continue use of the Services as contemplated under this Agreement or (b) replace or modify the Services to be non-infringing; provided that if (a) or (b) are not available to or economically feasible for Convercent, then Convercent will have the right to terminate each affected Order Form.

9. **Limitation of Liability**. EXCEPT BREACHES OF SECTION 5 (CONFIDENTIALITY), NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, FINES OR PENALTIES, COSTS OF PROCUREMENT OF SUBSTITUTE SERVICES OR TECHNOLOGY, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE LEGAL OR EQUITABLE THEORY ON THE BASIS OF WHICH ANY CLAIM FOR DAMAGES IS BROUGHT, INCLUDING, BUT NOT LIMITED TO, BREACH OF CONTRACT, TORT OR STATUTE, EVEN IF THE PARTY SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT WITH RESPECT TO BREACHES OF SECTION 5 (CONFIDENTIALITY) AND CONVERCENT'S OBLIGATIONS FOR INTELLECTUAL PROPERTY INFRINGEMENT PROVIDED IN SECTION 7.1, IN NO EVENT SHALL CONVERCENT'S LIABILITY TO CUSTOMER UNDER OR IN RESPECT OF THIS AGREEMENT EXCEED THE EQUIVALENT OF TWELVE (12) MONTHS OF FEES FOR SERVICES DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE LIABILITY.

10. **Compliance with Law.** In performing its obligations or exercising its rights under this Agreement, each party shall comply with all applicable laws and government regulations at all times, including but not limited to any applicable laws and regulations of the United States and other jurisdictions relating to export or re-export of technology, consumer protection, information access and privacy.

11. **Data Protection**.

11.1 **U.S. Law**. Customer acknowledges that Convercent is not, and Customer shall not take any action that would result in Convercent being or being deemed, a "business associate" as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Further, Customer represents and warrants to Convercent that Customer will not upload or transmit to the Services any content that (a) infringes, misappropriates or otherwise violates the rights of any third party, including intellectual property rights and

rights of privacy; (b) constitutes "protected health information" as defined by the HIPAA, or "cardholder data" or "sensitive authentication data" each as defined by the Payment Card Industry Data Security Standard, as amended or replaced from time to time ("Security Regulations"), and (c) otherwise would subject Convercent to or be in violation of the Security Regulations.

11.2 **Personal Data**. In the course of performing the Services for Customer, Convercent may receive and store information that can be used to uniquely identify, contact or locate a natural person, including but not limited to name, address, email address, or phone number ("Personal Data"). Convercent shall safeguard the confidentiality of Personal Data in accordance with Exhibit A, and will not access or use such Personal Information other than as necessary to perform the Services. Convercent receives and stores Personal Data solely as an agent acting on behalf of Customer.

11.3 **Security**. The Convercent product and modules are ISO 27001:2013 certified and Convercent will protect all Customer Data as described in Exhibit A.

11.4 **EU Data**. Convercent has certified that it complies with the US-EU Privacy Shield (www.privacyshield.gov), and will maintain such certification during the Term. With respect to processing any Customer Data that is Personal Data and originates from the European Economic Area ("EEA Personal Data"), Convercent will comply with the requirements of the Privacy Shield.

12. **General Provisions**.

12.1 The parties are independent contractors, and no agency, partnership, franchise, joint venture, or employment relationship is intended or created by this Agreement.

12.2 If any provision herein is held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force and effect without being impaired or invalidated in any way. The parties agree to replace any invalid provision with a valid provision that most closely approximates the intent and economic effect of the invalid provision.

12.3 Neither party shall be deemed to have waived any provision hereof unless such waiver is in writing and executed by a duly authorized officer of both parties. Except as otherwise set forth in this Agreement, no failure to exercise or delay in exercising any rights arising from this Agreement shall operate or be construed as a waiver thereof.

12.4 With the exception of any monetary obligations under this Agreement, neither party shall be responsible for performance of its obligations hereunder where delayed or hindered by events beyond its reasonable control, including, without limitation, acts of God or any governmental body, war or national emergency, riots or insurrection, sabotage, embargo, fire, flood, accident, strike or other labor disturbance, or interruption of or delay in systems, power or telecommunications under third-party control.

12.5 To be effective, any notice required to be given under this Agreement shall be given in writing, addressed to the applicable party (at the address in the Order Form) and hand delivered, which is effective upon delivery; sent by reputable overnight courier, which is effective on the business day following deposit with such courier; or sent by the United States mail, first class postage prepaid, which is effective on the third business day after deposit in the United States mail.

12.6 This Agreement will be governed and construed in accordance with the laws of the State of Colorado without giving effect to any principles that may provide for the application of the law of any other jurisdiction. Any legal suit, action or proceeding arising out of or related to this Agreement or the matters contemplated hereunder shall be instituted exclusively in the federal courts of the United States or the courts of the State of Colorado in each case located in the City of Denver, Colorado (except where such courts do not have jurisdiction), and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action or proceeding and waives any objection based on improper venue or forum non conveniens. In the event of litigation arising out of this Agreement, the prevailing party shall be entitled to its costs and reasonable attorneys' fees.

12.7 Neither party may assign this Agreement or any right, interest or benefit under this Agreement without the prior written consent of the other party; provided, however, either party may assign this Agreement to a successor who acquires substantially all of the assets or equity of such party through purchase, merger or other change in control transaction without the other party's consent. Any purported assignment in breach of the foregoing will be null and void. This Agreement will be fully binding upon, inure to the benefit of and be enforceable by the parties hereto and their respective successors and permitted assigns, and nothing in this Agreement confers upon any other person or entity any legal or equitable right whatsoever to enforce any provision of this Agreement.

12.8 This Agreement (together with any Order Forms) constitutes the entire agreement between the parties concerning the subject matter hereof and supersedes all prior and contemporaneous agreements and communications, whether oral or written, between the parties relating to the subject matter hereof, and all past courses of dealing or industry custom. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in a writing duly executed by authorized representatives of both parties.

Any standard terms associated with a Customer purchase order or other order document (e.g., general terms and conditions attached to the purchase order form) will be not binding on the parties and of no consequence whatsoever in interpreting the parties' legal rights and responsibilities as they pertain to Services provided under this Agreement. No such materials will be deemed to modify, add to, or supersede any provision of this Agreement. Neither party will have any obligations or liability to the other party with respect to any purchase orders that are not accepted by both parties. Similarly, any terms required to be accepted electronically through any Customer vendor enrollment, login, invoice submission, or other, process will not apply to this Agreement, are expressly rejected by the parties, and form no basis for any agreement between the parties; notwithstanding any indication of "agreement" to such terms, no such agreement is formed between the parties and the parties acknowledge that only authorized representatives of the parties may enter into agreements between the parties or amendments to this Agreement.

Exhibit A

Data Security

1. Purpose and Scope:

This Exhibit A, Data Security, (this "Exhibit") reflects the Parties' commitment to abide by the Applicable Laws and Regulations concerning the Processing of Customer Data, including Personal Data, provided by Customer in connection with Customer's execution of the Agreement. This Exhibit prescribes the minimum data protection and information security standards that Convercent, its agents or assigns meets and maintains in order to protect Customer Data and Customer systems from unauthorized use, access, disclosure, theft, manipulation, reproduction, Security Breach or otherwise during the term of the Agreement and for any period thereafter during which Convercent, its agents or its assigns has possession of or access to any Customer Data.

Capitalized terms used but not defined in this Exhibit shall have the meaning set forth in the Agreement. Convercent reserves the right to revise this Exhibit from time to time upon reasonable prior written notice and approval by Customer.

2. Definitions:

a. "Applicable Laws and Regulations" mean any applicable data protection, privacy or information security laws, codes and regulations or other binding restrictions governing Processing of Customer Data, including Personal Data, that are applicable to or required by (i) the Processing Location(s) identified in this Exhibit, or (ii) jurisdiction in which the Convercent or its Sub-Processors are located.

b. "Breach" or "Security Breach" means a compromise of the systems in which Customer Data has been accessed or acquired by one or more unauthorized parties or any act that violates any Applicable Laws and Regulations. For the avoidance of doubt, "a compromise of the systems" includes, but is not limited to: misuse, loss, destruction, or unauthorized access, collection, retention, storage, or transfer.

c. "Data Centers" means locations at which Convercent provides data Processing or transmission functions in support of this Agreement. Data Centers can be Convercent-owned or third party service model-based.

d. "Data Controller" means the party that determines the purposes of the Processing of Personal Data; for purposes of this Exhibit, Customer is the Data Controller.

e. "Data Processor" means the party that Processes Personal Data on behalf of, and under the instruction of, the Data Controller; for purposes of this Exhibit, Convercent is the Data Processor.

f. "Data Subject" means the identified or identifiable person who is the subject of Personal Data;

g. "Incident" means any impairment to the security of Customer Data, including, but not limited to: any (i) alleged or confirmed misuse of Personal Data; or (ii) unauthorized access to or attempt to access Customer Data.

h. "Industry Standard Encryption Algorithms and Key Strengths" means encryption should at least meet the following standard encryption algorithm (note: The algorithm and key strengths may change depending upon the new and most up-to-date industry standard encryption practice):

- Symmetric encryption: AES (≥ 128-bit);
- Asymmetric encryption: RSA (≥ 2048-bit);
- Hashing: SHA-2 (≥ 224-bit) with "salt" shall be added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings.

i. "Processing", "Processes" or "Process" means any operation or set of operations which is performed upon Customer Data, whether by automatic means or not, including but not limited to collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

j. "Processing Location" means the location(s) where the Personal Data is processed: worldwide.

k. "Restricted Data": Highly sensitive or regulated information that is intended only for a limited audience within Customer or whose release would likely have a material adverse financial or reputational effect on Customer, Customer employees, or Customer customers, Customer clients. All information in this category is restricted to a limited group with authorized need-to-know access. Examples include, but are not limited to: (i) Passwords, challenge/response answers, personal identification numbers (PIN), biometric data, and any other codes that provide access to systems or networks that store, transmit or process Customer Data; (ii) Government issued identification numbers (e.g., Social Security number; driver's license number; state identification number); (iii) Financial and Payment Information (e.g., bank account numbers, credit card or debit card numbers); (iv) employee or customer date of birth; (v) Pre-release financial information; (vi)

Information related to non-public mergers and acquisitions; and (vii) medical health records about an individual;

l. "Sub-processor" means any Affiliate, agent or assign of Convercent that may Processes Personal Data pursuant to the terms of the Agreement, and any unaffiliated Data Processor engaged by Convercent or by an Affiliate of Convercent.

3. Security Management:

3.1 Scope and Contents. Convercent will develop, implement, maintain and enforce a written information privacy and security program ("Security Program") that (i) complies with ISO 27001, (ii) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data and (iii) is appropriate to the nature, size and complexity of Convercent's business operations; and (iv) complies with any Applicable Laws and Regulations that are applicable for the geographic region in which Convercent does business.

a. Security Program Changes. Convercent will provide details of any major changes to its Security Program that may adversely affect the security of any Customer Data.

b. Security Officer. Convercent will designate a senior employee to be responsible for overseeing and carrying out its Security Program and for communicating with Customer on information security matters (the "Convercent's Security Officer"). Upon Customer's request, the Convercent Security Officer will provide Customer with the contact information of one or more Convercent representatives who will be available to discuss any security concerns (e.g., discovered vulnerability, exposed risk, reported concern) with Customer and to communicate the level of risk associated with such concerns and any remediation thereof. A representative must be available during normal business hours.

3.2 Personnel Security.

a. Verification Checks. Prior to assigning any of its Personnel to positions in which they will, or Convercent reasonably expects them to, have access to Customer Data, Convercent will conduct or verify background checks on such Personnel, except where expressly prohibited by law. For the purposes of this Exhibit, "Personnel" means Convercent's employees, independent contractors, and subcontractors.

b. Training. Convercent Personnel will, upon hiring, and at least annually thereafter, participate in security awareness training. This training will cover, at a minimum, Convercent's security policies, including acceptable use, password protection, data classification, Incident and Breach reporting, the repercussions of violations, and brief overviews of Applicable Laws and Regulations.

c. Due Diligence over Subcontractors. Convercent maintains a security process to conduct appropriate due diligence prior to utilizing subcontractors to provide any of the Services. Convercent will assess the security capabilities of any such subcontractors on an annual basis to ensure subcontractor's ability to comply with this Exhibit and the terms of the Agreement. The due diligence process will provide for the identification and resolution of significant security issues prior to engaging a subcontractor, written information security requirements that oblige subcontractor to adhere to Convercent's key information security policies and standards within all contracts, and for the identification and resolution of any security issues during the term of the Agreement.

4. Physical Security:

4.1 General. The physical security processes in this Article 4 apply to all facilities used to provide the Services at which Customer Data is accessed, processed, stored, transferred or maintained, including any floor space where Services are performed in which Personnel have access to Customer Data and servers or other equipment that processes or stores Customer Data (the "Secure Area").

4.2 Secure Area. Customer Data will only reside within a Secure Area. Convercent will restrict access to and will control and monitor all physical areas in Convercent's premises that contain Customer Data. Convercent will secure and monitor access to any Secure Area, and will maintain physical security controls at the Secure Area, on a 24-hours-per-day, 7-days-per-week basis ("24/7"). Convercent will revoke any Personnel's access to Secure Areas within twenty-four (24) hours of the cessation of such Convercent Personnel's need to access buildings, system(s) or application(s).

4.3 Data Centers. To the extent Convercent is operating a Data Center or utilizing a Third Party Data Center, Convercent will comply with physical security controls outlined in industry standards such as ISO 27001, SSAE 16 or ISAE 3402, or PCI-DSS. All access to areas, cabinets, or racks that house telecommunications, networking devices and other "data transmission lines" or equipment will be controlled as follows:

a. access will be controlled by badge reader at one or more entrance points;

b. doors used only as exit points will have only "one way" doorknobs or crash bar exit devices installed;

c. all doors will be equipped with door alarms contacts;

d. all exit doors will have video surveillance capability; and

e. all card access and video surveillance systems will be tied into generator or UPS backup systems.

5. Logical Security:

5.1 General. The logical security processes in this Article 5 apply to all Convercent's systems or Convercent's agents' or its assigns' systems and supporting networks used to provide the Services on which Customer Data is accessed, processed, stored, transferred or maintained.

5.2 Systems Access Control and Network Access Control.

a. Access Controls. Convercent certifies that it employs access control mechanisms that:

i. prevent unauthorized access to Customer Data;

ii. limit access to Personnel with a business need to know;

iii. follow principle of least privilege allowing access to only the information and resources that are necessary under the terms of the Agreement; and

iv. have the capability of detecting, logging, and reporting access to the system or network or attempts to breach security of the system or network.

b. Accounts. All Personnel must have an individual account that authenticates that individual's access to Customer Data. Convercent does not allow sharing of accounts. Access controls and passwords are configured in accordance with industry standards and best practices. Passwords will be hashed with industry standard algorithms per Article 10 below.

c. Regular Review of Access Controls. Convercent maintains a process to review access controls on a minimum annual basis for all Convercent systems that contain Customer Data, including any system that, via any form of communication interface, can connect to the system on which Customer Data is stored. These access processes and the process to establish and delete individual accounts will be documented in, and will be in compliance with, Convercent's security policies and standards referenced in Article 3.1 above. Convercent maintains the same processes of review and validation for any third party hosted systems it uses that contain Customer Data.

d. Remote Access Authentication. Convercent will configure remote access to all networks storing or transmitting containing Customer Data to require two-factor authentication for such access or at a minimum will use Access Control Lists ("ACLs") to only allow connectivity to such networks from Convercent's own network.

e. Revocation of Access. Convercent will revoke Personnel's access to physical locations, systems, and applications that contain or process Customer Data within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s).

5.3 Telecommunication and Network Security.

a. Firewalls. Convercent will deploy reasonably appropriate firewall technology in the operation of the Convercent's sites. Traffic between Customer and Convercent will be protected and authenticated by industry standard cryptographic technologies. Specifically, firewall(s) must be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing.

b. Firewall Maintenance. At a minimum, Convercent will review firewall rule sets annually to ensure that legacy rules are removed and active rules are configured correctly.

c. Intrusion Detection and Prevention. Convercent will deploy intrusion detection or preferably prevention systems (NIDS/NIPS) in order to generate, monitor, and respond to alerts which could indicate potential compromise of the network and/or host.

d. Log Management. Convercent shall deploy a log management solution and retain logs produced by firewalls and intrusion detection systems for a minimum period of one (1) year.

e. Network Segmentation. Convercent shall establish and maintain appropriate network segmentation, including the use of virtual local area networks (VLANS) where appropriate, to restrict network access to systems storing Customer Data. Convercent will proxy all connections from public networks into the Convercent's internal network using DMZ or equivalent. Convercent will not allow direct connections from public networks into any network segment storing Customer Data.

f. Wireless Security. If Convercent deploys a wireless network, Convercent will maintain written policies governing the use, configuration and management of wireless networks:

i. Physical Access – All wireless devices shall be protected using appropriate physical controls to minimize the risk of theft, unauthorized use, or damage;

ii. Network Access – Network access to wireless networks should be restricted only to those authorized;

iii. The service set identifier (SSID), administrator user ID, password and encryption keys shall be changed from the default value;

iv. Encryption of all wireless connections will be enabled using Industry Standard Encryption Algorithms (i.e. WPA2/WPA with 802.1X authentication and AES encryption). WEP should never be used;

v. If supported, auditing features on wireless devices shall be enabled and resulting logs shall be reviewed periodically by designated staff or a wireless intrusion prevention system. Logs should be retained for ninety (90) days or longer; and

vi. SNMP shall be disabled if not required for network management purposes. If SNMP is required for network management purposes, SNMP will be read-only with appropriate access controls that prohibit wireless devices from requesting and retrieving information and all default community strings will be changed.

g. Rogue Access Point Detection. Convercent will maintain a program to detect rogue access points at least quarterly to ensure that only authorized wireless access points are in place. If Convercent has not deployed a wireless solution, they are still required to conduct this quarterly audit to ensure that user-deployed wireless access points are not in use.

5.4 Malicious Code Protection.

a. All workstations and servers will run the current version of industry standard anti-virus software with the most recent updates available on each workstation or server. Virus definitions must be updated within twenty-four (24) hours of release by the anti-virus software vendor. Convercent will configure this equipment and have supporting policies to prohibit users from disabling anti-virus software, altering security configurations, or disabling other protective measures put in place to ensure the safety of Customer's or Convercent's computing environment.

b. Convercent will have current anti-virus software configured to run real-time scanning of machines and a full system scan on a regularly scheduled interval not to exceed seven (7) calendar days.

c. Convercent will scan incoming and outgoing content for malicious code on all gateways to public networks, including, but not limited to, email and proxy servers.

d. Convercent will quarantine or remove files that have been identified as infected and will log the event.

5.5 Data Loss Prevention. Convercent will employ a system to prevent the inadvertent or intentional compromise of Customer Data. This centralized system should monitor data in motion. Controls must exist to track activity, inspect network traffic, including email and other protocols, and filter/block certain user actions to ensure Customer Data remains secured.

6. Systems Development and Maintenance:

6.1 Documentation. Convercent will maintain documentation on overall system, network, and application architecture, data flows, process flows, and security functionality for all applications that process or store any Customer Data.

6.2 Change Management. Convercent will employ an effective, documented change management program with respect to the Services as an integral part of its security profile. This includes logically or physically separate environments from production for all development and testing. No Customer Data will be transmitted, stored or processed in an environment that does not maintain at least the minimum administrative, technical and physical safeguards as described in this Exhibit.

6.3 Vulnerability Management and Application Security Assessments. Convercent will run internal and external network vulnerability scans at least quarterly and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades). Vulnerabilities identified and rated as high risk by the Convercent will be remediated within ninety (90) days of discovery.

a. For all Internet-facing applications that collect, transmit or display Customer Data, Convercent agrees to conduct an application security assessment review to identify common security vulnerabilities as identified

by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security, including, but not limited to, a static code analysis or penetration test of the application, as well as a code review. At a minimum, it will cover the OWASP Top 10 vulnerabilities (https://www.owasp.org).

b. Convercent may utilize a qualified third party to conduct the application security assessments. Convercent may conduct the security assessment review themselves, provided that Convercent's Personnel performing the review are sufficiently trained, follow industry standard best practices, and the assessment process is reviewed and approved by Customer. Vulnerabilities identified and rated as high risk by the Convercent will be remediated within ninety (90) days of discovery.

6.4 Source code review. Convercent will have a documented program for secure code reviews and maintain documentation of secure code reviews performed for all applications that store or process Customer Data.

6.5 Patch Management. Convercent will patch all workstations and servers with all current operating system, database and application patches deployed in Convercent's computing environment according to a schedule predicated on the criticality of the patch. Convercent will perform appropriate steps to help ensure patches do not compromise the security of the information resources being patched. All emergency or critical rated patches must be applied as soon as possible but at no time will exceed six weeks from the date of release.

7. Email Security:

If Convercent is sending emails to Customer customers or employees, appropriate email identity solutions, including but not limited to DKIM, SPF, and DMARC, will be utilized.

8. Customer Security Assessments and Audits:

8.1 Convercent agrees, upon written request no more than on an annual basis, to allow its procedures and documentation to be inspected by Customer (or its designee) in order to ascertain compliance with Applicable Laws and Regulations, this Exhibit, or any non-disclosure agreements and any agreements between Customer and Convercent.

8.2 Convercent shall reasonably cooperate with audit requests by providing access to relevant knowledgeable personnel, documentation, and application software.

9. Incident Response and Notification Procedures:

9.1 Convercent will maintain an Incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of Incidents. Upon discovering or otherwise becoming aware a Breach, Convercent shall take all reasonable measures to mitigate the harmful effects of the Breach. Convercent shall also notify Customer of the Breach as soon as practicable, but in no event later than 48 hours after the Breach. Notice to Customer shall include: (i) the identification of the Customer Data which has been or Convercent reasonably believes has been used, accessed, acquired or disclosed during the incident; (ii) a description of what happened, including the date of the incident and the date of discovery of the incident, if known; (iii) the scope of the incident, including a description of the type of Customer Data involved in the incident; (iv) a description of Convercent's response to the incident, including steps Convercent has taken to mitigate the harm caused by the incident; and (v) other information as Customer may reasonably request and is reasonably applicable. Convercent agrees to cover the costs of any such notification, including reimbursing Customer for any reasonable costs.

9.2 Convercent will retain all data related to known and reported Incidents or investigations indefinitely or until Customer notifies Convercent that the image is no longer needed. Upon Customer's request, Convercent will permit Customer or its third party auditor to review and verify relevant video surveillance records, access logs and data pertaining to any Incident investigation. Upon conclusion of investigative, corrective, and remedial actions with respect to an Incident, Convercent will prepare and deliver to Customer a final report that describes in detail: (i) the extent of the Incident; (ii) the Customer Data disclosed, destroyed, or otherwise compromised or altered; (iii) all supporting evidence, including, but not limited to, system, network, and application logs; (iv) all corrective and remedial actions completed; and (v) all efforts taken to mitigate the risks of further Incidents.

10. Storage, Handling and Disposal:

10.1 Data Segregation. Convercent will physically or logically separate and segregate Customer Data from its other clients' data.

10.2 Electronic Form Data. Convercent will utilize Industry Standard Encryption Algorithms and Key Strengths (as defined in the "Definitions" section of this Exhibit) to encrypt the following:

a. All Customer Data that is in electronic form while in transit over all public wired networks (e.g., Internet) and all wireless networks.

b. All Customer Data while In Storage. "In Storage" means information stored in databases, in file systems, and on various forms of online and offline media (DASD, tape, etc.) and is also commonly referred to as "at rest."

c. Passwords for privileged access will be hashed with irreversible industry standard algorithms with randomly generated "salt" added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings. The randomly generated salt should be at least as long as the output of the hash function.

d. If mobile devices (e.g., laptop, cell phone, tablet) are used to perform any part of the Services, Convercent will encrypt all Customer Data on such mobile devices.

10.3 Key Management. Where encryption is utilized, Convercent will maintain a key management process that meets the following minimum requirements:

a. At least one key custodian must be officially designated.

b. Key custodians must ensure that all keys used in a storage encryption solution are secured and managed properly to support the security of the solution.

c. Key management must be planned to include secure key generation, use, storage and revocation.

d. Key management practices must support the recovery of encrypted data if a key is inadvertently disclosed, destroyed or becomes unavailable.

e. Key custodians must ensure that access to encryption keys is properly restricted to approved administrators. Private keys must not be stored on the same media and/or virtual instance as the data they protect.

f. Authentication must be required in order to gain access to keys.

g. Keys should be rotated annually and must be replaced before they expire.

10.4 Physical Form Data. Convercent will only store Customer Data in physical form in a Secure Area, and Convercent will establish and operate a document control system to record and track the transfer of all Customer Data that is in physical form both (i) between and within Convercent facilities, and (ii) via any external shipment. Such a control system will include, at minimum, a description of the specific records being transferred (e.g., customer or employee records, etc.), as well as the parties who are preparing, shipping, receiving, and processing such materials.

10.5 Shipments. Convercent will transfer all Customer Data in physical form (i.e. external hard drives, backup tapes, etc.) in secure containers or packaging. Convercent will ship any Customer Data in physical form via controlled transportation methods reasonably designed to prevent unauthorized access or compromise, including encryption of electronic media where applicable. Controlled transportation methods include enclosed locked vehicles, registered mail, and commercial shipping services with numbered tracking capability (e.g., UPS, FedEx).

10.6 Data Retention. Except where prohibited by law, upon (i) the date of expiration or termination of the Agreement; (ii) when Customer Data is no longer required for the purposes of the Agreement; or (iii) at any time upon written request from Customer, whichever occurs earliest:

a. Convercent will promptly remove the Customer Data from Convercent's environment and destroy it within a reasonable timeframe, but in no case longer than thirty (30) days thereafter, with the exception of encrypted backups in Microsoft Azure which are deleted in according to Convercent policy.

b. all media used to store Customer Data will be sanitized or destroyed as required in Article 10.7, and

c. Convercent will provide Customer with a written certification regarding such removal, destruction, and/or cleaning upon request.

10.7 Destruction of Data. Convercent will dispose of Customer Data when information is deemed no longer necessary to preserve as outlined in Article 10.6, or has exceeded industry best practices for the time/duration/age of the Customer Data. Customer Data should be disposed of in a method that prevents any recovery of the data in accordance with industry best practices for shredding of physical documents and wiping of electronic media (e.g. NIST SP 800-88r1). Convercent will destroy any equipment containing Customer Data that is damaged or non-functional. All Customer Data must be rendered unreadable and unrecoverable regardless of the form (physical or electronic).

11.Ownership; Use:

Convercent acknowledges and agrees that it has no ownership of, or right to use, Customer Data other than as expressly permitted under the Agreement or as authorized by Customer in writing. For the avoidance of doubt, Convercent has no right to copy, use, reproduce, display, perform, modify or transfer Customer Data or any derivative works thereof, except as expressly provided in the Agreement or as expressly authorized by Customer in writing. Convercent acknowledges and agrees that it will not use (or permit any third party to use) the Customer Data for any use other than as expressly provided in the Agreement.

11. Business Continuity and Disaster Recovery:

Convercent will set up a Business Continuity Management program that meets the needs of the business and Services being provided to Customer. To that end, a minimum level of crisis management, business continuity, and disaster recovery planning should be completed by Convercent.

a. Business Continuity, and Disaster Recovery Plans shall be as follows:

- A Business Continuity Plan includes, but is not limited to, elements such as event management, life safety, business recovery, alternative site locations, and call tree testing.
- A Disaster Recovery Plan includes, but is not limited to, infrastructure, technology, and system(s) details, recovery activities, and identifies the people / teams required for such recovery.

b. Plan Content. Plan documentation in Article 12(a) will address actions that Convercent will take in the event of an extended outage of Service and will include test results for the Business Continuity and Disaster Recovery Plan from a test performed in the immediately preceding twelve (12) months. Convercent will ensure that their plans will address the actions and resources required to provide for (i) the continuous operation of Convercent, and (ii) in the event of an interruption, the recovery of the functions required to enable Convercent to provide the Services described in the Agreement, including all required systems, hardware, software, resources, personnel and data supporting these functions, within duration of time (the "Recovery Time Objective") sufficient to meet any service levels described in the Agreement.

12. Survival:

Convercent's obligations and Customer's rights under this Exhibit shall become effective on the Effective Date of the Agreement and will continue in effect so long as Convercent possesses Customer Data.

13. Conflict:

If and to the extent language in this Exhibit or any of its Schedule conflicts with the Agreement, this Exhibit shall control.

14. Processing of Personal Data:

The following additional terms shall apply if Convercent will Process Personal Data in connection with its execution of the Agreement:

14.1 Processing Instructions: Convercent shall Process Personal Data only to deliver services to Customer in accordance with its written instructions (unless expressly waived in a written requirement) provided during the term of the Agreement. In the event Convercent reasonably believes there is a conflict amongst Applicable Laws and Regulations or that Customer's instructions conflict with any Applicable Laws and Regulations, Convercent will inform Customer immediately and shall cooperate in good faith to resolve the conflict and achieve the goals of such instruction.

14.2 Use of Sub Processors:

Customer hereby consents to the Convercent's use of the following subprocessors as set out below:

Subprocessor	Brief Description of Processing
Five Star Call Centers	Call Center – Helpline/Call Center Services
Amazon Web Services	Data Center – Failover Cloud Environment
Microsoft Azure	Data Center – Primary Cloud Environment
Datavail	Database Administration – 24/7 Database Monitoring

14.3 Transfer of Personal Data: Convercent shall not cause or permit any Personal Data to be transferred outside of the Processing Location(s) identified in this Exhibit without Customer's prior written consent. For the avoidance of doubt, this transfer restriction does not pertain to Customer personnel who have access to Personal Data and Convercent shall not be held responsible for actions of Customer personnel.

14.4 Limitation on Disclosure of Personal Data: To the extent legally permitted, Convercent shall promptly notify Customer in writing upon receipt of an order, demand, or document purporting to request, demand or compel the production of Personal Data to any third party. To the extent legally permitted, Convercent shall not disclose Personal Data to the third party without providing Customer at least forty-eight (48) hours' notice, so that Customer may, at its own expense, exercise such rights as it may have under Applicable Laws and Regulations to prevent or limit such disclosure. Notwithstanding the foregoing, Convercent will exercise commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of Personal Data; additionally, Convercent will use reasonable efforts

to cooperate with Customer with respect to any action taken pursuant to such order, demand, or other document request, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Personal Data.

14.5 Compliance with Applicable Laws and Regulations: Convercent shall Process Personal Data in accordance with Applicable Laws and Regulations of the Processing Location(s) identified in this Exhibit. Convercent represents and warrants that Convercent will maintain privacy policies sufficient to protect the Personal Data and compliant with the Applicable Laws and Regulations of the Processing Location(s) identified in this Exhibit.