MASTER DATA PROTECTION AGREEMENT

This MASTER DATA PROTECTION AGREEMENT (“MDPA”) is entered into by and between Zipper Athletics Inc whose registered office is at _____ and its Affiliates, if any, ("Zipper"), and Supplier and its Affiliates (“Supplier”), (together “Parties”).This MDPA is governed by the terms of the applicable agreement entered into by and between the Parties for the supply of Products and/or Services by Supplier to Zipper (“the Agreement”). In the event of a conflict between this MDPA, including any attachments herein, and the Agreement, the provisions of this MDPA will control but only with respect to the subject matter hereof.

In consideration of the mutual promises and covenants hereinafter contained and of other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1.0 SCOPE OF AGREEMENT. This MDPA is comprised of these General Terms and the following

Attachments A-D attached herein, which are incorporated by reference:

1. Attachment A INFORMATION SECURITY EXHIBIT
2. Attachment B DATA PROTECTION EXHIBIT
3. Attachment C BUSINESS ASSOCIATE AGREEMENT
4. Attachment D STANDARD CONTRACTUAL CLAUSES
5. Attachment E GLOSSARY

2.0 GENERAL TERMS

2.1 Choice of Law. The validity, interpretation, and performance of this MDPA shall be governed by and construed under the laws of the State of Delaware, United States of America, as if performed wholly within the state and without giving effect to the principles of conflicts of law. The Federal District Courts in the State of Delaware shall have exclusive jurisdiction over any claim arising under this MDPA, provided that either Party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such Party’s intellectual property or proprietary rights. The Parties agree that the UN Convention on Contracts for the International Sale of Goods shall not apply to the interpretation or enforcement of this MDPA.

2.2 Attorneys’ Fees. In any suit or proceeding relating to this MDPA the prevailing Party will have the right to recover from the other its costs and reasonable fees and expenses of attorneys, accountants, and other professionals incurred in connection with the suit or proceeding, including costs, fees and expenses upon appeal, separately from and in addition to any other amount included in such judgment. This provision is intended to be severable from the other provisions of this MDPA, and shall survive expiration or termination and shall not be merged into any such judgment.

2.3 No Waiver. The waiver by either party of any right provided under this MDPA shall not constitute a subsequent or continuing waiver of such right or of any other right under this MDPA.2.4 Assignment. Unless otherwise expressly provided under this MDPA, neither Party may assign this MDPA or assign its rights or delegate its obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other Party. Any attempt at such an assignment or delegation without the other's Party's written consent will be void. The rights and liabilities of the parties under this MDPA will bind and inure to the benefit of the Parties' respective successors and permitted assigns.For purposes of this Section

2.4 (Assignment), a twenty percent (20%) change in control of a Party shall constitute an assignment.

2.5 Severability. If one or more terms of this MDPA become or are declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, each such part or term shall be null and void and shall be deemed deleted from this MDPA. All remaining terms of this MDPA shall remain in full force and effect. However, if this paragraph is invoked and, as a result, the value of this MDPA is materially impaired for either Party, then the affected Party may terminate this MDPA by written notice with immediate effect.

2.6 Notices. All notices required or permitted under this MDPA shall be in writing. Notices will be deemed to have been given (i) one day after deposit with a commercial express courier specifying next day delivery; or (ii) two days for international courier packages specifying two-day delivery, with written verification of receipt. All communications shall be sent to the Parties' addresses shown on the first page of this MDPA or to such other address as may be designated from time to time by a Party by giving at least fourteen (14) days' written notice to the other Party.

2.7 Survival. This section 2.0 shall survive the expiration or earlier termination of this Agreement. This MDPA is the complete agreement between the Parties concerning the subject matter of this MDPA and replaces any prior oral or written communications between the Parties. This MDPA is subject to the terms and conditions of the Agreement, including, but not limited to any limitations or exclusions of liability set forth in the Agreement. This MDPA, together with the Agreement, comprises the complete agreement between the Parties. There are no conditions, understandings, agreements, representations, or warranties expressed or implied, that are not specified herein. This MDPA may only be modified by a written document executed by the Parties hereto. The Parties, by signing below, confirm that they have read, understood, and expressly approve of the terms and conditions of this MDPA. The Supplier's obligations under this MDPA will terminate when the Supplier no longer holds, Processes, or otherwise has access to Protected Data.

ATTACHMENT A INFORMATION SECURITY EXHIBIT

1. Scope

This Information Security Exhibit (“ISE”) applies to the extent that Supplier Processes or has access to Protected Data in the Performance of its obligations to the Zipper. This ISE outlines the information security requirements between Zipper and Supplier and describes the technical and organizational security measures that shall be implemented by the Supplier to secure Protected Data prior to the Performance of any Processing under the Agreement.Unless otherwise stated, in the event of a conflict between the Agreement and this ISE, the terms of this ISE will control as it relates to the Processing of Protected Data.All capitalized terms not defined in the Glossary have the meanings set forth in the Agreement.

2. General Security Practices

Supplier has implemented and shall maintain appropriate technical and organizational measures designed to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this ISE for its personnel, equipment, and facilities at the Supplier’s locations involved in Performing any part of the Agreement.

3. General Compliance

a. Compliance. Supplier shall document and implement processes and procedures to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by Supplier. The Supplier shall implement and operate information security in accordance with the Supplier’s own policies and procedures, which shall be no less strict than the information security requirements set forth in this ISE.
b. Protection of records. Supplier shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.
c. Review of information security. Supplier’s approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures) shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.
d. Compliance with security policies and standards. Supplier’s management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.
e. Technical compliance review. Supplier shall regularly review information systems for compliance with Supplier’s information security policies and standards.
f. Information Risk Management (“IRM”). Supplier shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Supplier is required to have a risk management framework and conduct periodic (i.e., at least annual) risk assessments of its

environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks.Threat and vulnerability assessment must be periodically reviewed and prompt remediation actions taken where material weaknesses are found. Supplier will provide Zipper with relevant summary reports and analysis upon written request, provided the disclosure of which would not violate Supplier's own information security policies, or Applicable Laws.

4. Technical and Organizational Measures for Security

a. Organization of Information Security
i. Security Ownership. Supplier shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.
ii. Security Roles and Responsibilities. Supplier shall define and allocate information security responsibilities in accordance with Supplier's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.
iii. Project Management. Supplier shall address information security in project management to identify and appropriately address information security risks.
iv. Risk Management. Supplier shall have a risk management framework and conduct periodic (i.e., at least annual) risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Protected Data.

b. Human Resources Security
i. General. Supplier shall ensure that its personnel are under a confidentiality agreement that includes the protection of Protected Data and shall provide adequate training about relevant privacy and security policies and procedures. Supplier shall further inform its personnel of possible consequences of breaching Supplier's security policies and procedures, which must include disciplinary action, including possible termination of employment for Supplier's employees and termination of contract or assignment for Representatives and temporary personnel.
ii. Training. Supplier personnel with access to Protected Data shall receive appropriate, annual periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training shall be provided before Supplier personnel are granted access to Protected Data or begin providing services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.
iii. Background Checks. In addition to any other terms in the Agreement related to this subject matter, Supplier shall conduct criminal and other relevant background checks for its personnel in compliance with Applicable Laws and the Supplier's policies.

c. Trusted Device Standards.
i. Supplier personnel shall:

A. Only use trusted Devices that are configured with security software (i.e., anti-virus, anti-malware, encryption, etc.);
B. Follow trusted device standards when accessing Protected Data or when having Protected Data in their possession, custody, or control. The trusted device standard specifies the requirements that user devices ("Devices") must satisfy to be trusted when Processing Protected Data whether or not connected to a Zipper's network through wired, wireless, or remote access (the "Network"). Devices that fail to comply with this standard will not be entitled to access Network unless Zipper determines limited access is acceptable. Zipper's Network access policies establish requirements for physical and wireless network data ports that provide local network communications and telephony services.

ii. Trusted device standards include, at a minimum, the following:
A. Each Device must be uniquely associated with a specific, individual user;
B. Devices must be configured for automatic patching. All operating system and application security patches must be installed within the timeframe recommended or required by the issuer of the patch, in any event, no later than four (4) weeks of the general release of such patch by the issuer.
C. Devices must be encrypted (i.e., full disk, endpoint encryption) and secured with a protected (e.g., password, PIN, finger print, facial recognition, biometrics, etc.) screen lock with the automatic activation feature set to ten (10) minutes or less. Users must lock the screen or log off when the device is unattended;
D. Devices must not be rooted or jailbroken;
E. Devices must be periodically scanned for restricted or prohibited software (e.g., certain prohibited peer-to-peer sharing and social media apps that have been found to exploit/exfiltrate data); and
F. Devices must run an acceptable industry standard anti-malware solution. On-access scan and automatic update functionality must be enabled.

iii. Implement policies designed to prevent the storage of Protected Data on unencrypted smartphones, tablets, USB drives, DVD/CDs, or other portable media without prior written authorization from Zipper;
and take measures to prevent accidental exposure of Protected Data (e.g., using privacy filters on laptops).

d. Personnel Access Controls

i. Access.
A. Limited Use. Supplier understands and acknowledges that Zipper may be granting Supplier access to sensitive and proprietary information and computer systems in order for the Supplier to Perform its obligations to the Zipper. Supplier will not
(i) access the Protected Data or computer systems for any purpose other than as necessary to Perform its obligations to Zipper; or
(ii) use any system access information or log-in credentials to gain unauthorized access to Protected Data or Zipper's systems, or to exceed the scope of any authorized access.

B. Authorization. Supplier shall restrict access to Protected Data and systems at all times solely to those Representatives whose access is necessary to Performing Supplier's obligations to the Zipper.
C. Suspension or Termination of Access Rights. At Zipper's reasonable request, Supplier shall promptly and without undue delay suspend or terminate the access rights to Protected Data and systems for any Supplier's personnel or its Representatives reasonably suspected of breaching any of the provisions of this ISE; and Supplier shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.
D. Information Classification. Supplier shall classify, categorize, and/or tag Protected Data to help identify it and to allow for access and use to be appropriately restricted.
ii. Access Policy. Supplier shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Supplier shall maintain a record of security privileges of its personnel that have access to Protected Data, networks, and network services. Supplier shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.e.

Access Authorization.
i. Supplier shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Zipper's systems and networks. Supplier shall use an enterprise access control system that requires revalidation of its personnel by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.
ii. Supplier shall maintain and update a record of personnel authorized to access systems that contain Protected Data and Supplier shall review users' access rights at regular intervals.
iii. For systems that process Protected Data, Supplier shall revalidate (or where appropriate, deactivate) access of users who change reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.
iv. Supplier shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

f. Network Design. For systems that process Protected Data, Supplier shall have controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.
g. Least Privilege. Supplier shall limit access to Protected Data to that personnel with Performance obligations and, to the extent technical support is needed, its personnel performing such technical support.
h. Authentication
i. Supplier shall use industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords/PINs, Supplier shall require that the passwords/PINs are renewed and changed regularly, at least every 180 days.

ii. Where authentication mechanisms are based on passwords, Supplier shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).
iii. Supplier shall ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals.
iv. Supplier shall monitor repeated failed attempts to gain access to the information system.
v. Supplier shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.
vi. Supplier shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

i. Cryptography
i. Cryptographic controls policy

A. Supplier shall have a policy on the use of cryptographic controls based on assessed risks.
B. Supplier shall assess and manage the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecate and disallow usage of weak cypher suites and insufficient bit and block lengths.
C. Supplier's cryptographic controls/policy shall address appropriate algorithm selections, key management, and other core features of cryptographic implementations.

ii. Key management. Supplier shall have procedures for distributing, storing, archiving, and changing/updating keys; recovering, revoking/destroying, and dealing with compromised keys; and logging all transactions associated with such keys.
j. Physical and Environmental Security
i. Physical Access to Facilities

A. Supplier shall limit access to facilities where systems that Process Protected Data are located to authorized individuals.
B. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.
C. Facilities shall be monitored and access-controlled at all times (24x7).
D. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data. Supplier must register personnel and require them to carry appropriate identification badges.

ii. Physical Access to Equipment. Supplier equipment used to process or store Protected Data shall be protected using industry standard process to limit access to authorized individuals.
iii. Protection from Disruptions. Supplier shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.iv. Clear Desk.

Supplier shall have policies requiring a “clean desk/clear screen” to prevent inadvertent disclosure of Protected Data.k. Operations Security

i. Operational Policy. Supplier shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. Supplier shall communicate its policies and requirements to all persons involved in the Processing of Protected Data. Supplier shall implement the appropriate management structure and control designed to ensure compliance with such policies and with Applicable Laws concerning the protection and Processing of Protected Data.
ii. Security and Processing Controls.

A. Areas. Supplier shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks and services that store or Process Protected Data.
B. Standards and Procedures. Such standards and procedures shall include: security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

iii. Logging and Monitoring. Supplier shall maintain logs of administrator and operator activity and data recovery events related to Protected Data.

l. Communications Security and Data Transfer

i. Networks. Supplier shall, at a minimum, use the following controls to secure its networks that access or Process Protected Data:

A. Network traffic shall pass through firewalls, which are monitored at all times. Supplier must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.
B. Network devices used for administration must utilize industry standard cryptographic controls when Processing Protected Data.
C. Anti-spoofing filters and controls must be enabled on routers.
D. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 12 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days; or utilize other strong log-in credentials (e.g., biometrics).
E. Initial user passwords are required to be changed at first log-on. Supplier shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.
F. Firewalls must be deployed to protect the perimeter of Supplier’s networks.

ii. Virtual Private Networks (“VPN”). When remote connectivity to the Disclosing or Supplier’s network is required for Processing of Protected Data:
A. Connections must be encrypted using industry standard cryptography (i.e., a minimum of 256-bit encryption).

B. Connections shall only be established using VPN servers.
C. The use of multi-factor authentication is required.

iii. Data Transfer. Supplier shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of this ISE. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

m. System Acquisition, Development, and Maintenance
i. Security Requirements. Supplier shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.
ii. Development Requirements. Supplier shall have policies for secure development, system engineering, and support. Supplier shall conduct appropriate tests for system security as part of acceptance testing processes. Supplier shall supervise and monitor the activity of outsourced system development.

n. Penetration Testing and Vulnerability Scanning & Audit Reports
i. Testing. Supplier will perform periodic penetration tests on their internet perimeter network. Audits will be conducted by the Supplier's compliance team using industry recommended network security tools to identify vulnerability information. Upon written request from Zipper, Supplier shall provide a Vulnerability & Penetration testing report at the organization level which may include an executive summary of the results and not the details of actual findings.
ii. Audits. Supplier shall respond promptly to and cooperate with reasonable requests by Zipper for security audit, scanning, discovery, and testing reports.
iii. Remedial Action. If any audit or penetration testing exercise referred to in Section 4 (n)(ii), above reveals any deficiencies, weaknesses, or areas of non-compliance, Supplier shall promptly take such steps as may be required, in Supplier's reasonable discretion, to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances and in any case within three (3) months of the findings from the audit and/or test.
iv. Status of Remedial Action. Upon request, Supplier shall keep Zipper informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Zipper as soon as may be practicable given the circumstances that all necessary remedial actions have been completed.

o. Contractor Relationships
i. Policies. Supplier shall have information security policies or procedures for its use of Representatives that impose requirements consistent with this ISE. Such policies shall be reviewed at planned intervals or if significant changes occur. Agreements with Representatives shall include requirements that are consistent with, or analogous to, this MDPA.
ii. Monitoring. Supplier shall monitor and audit service delivery by its Representatives and review its Representatives' security practices against the security requirements set forth in

Supplier's agreements with such Representatives. Supplier shall manage changes in Representative services that may have an impact on security.

p. Management of Information Security Incidents and Improvements
i. Responsibilities and Procedures. Supplier shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.
ii. Reporting Information Security Incident. Supplier shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as reasonably possible. All employees and Representatives should be made aware of their responsibility to report Information Security Incidents as quickly as reasonably possible.
iii. Reporting Information Security Weaknesses. Supplier, employees, and Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.
iv. Assessment of and Decision on Information Security Events. Supplier shall have an incident classification scale in place in order to decide whether a security event should be classified as an Information Security Incident. The classification scale should be based on the impact and extent of an incident.
v. Response Process. Supplier shall maintain a record of Information Security Incidents with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

q. Information Security Aspects of Business Continuity Management
i. Planning. Supplier shall maintain emergency and contingency plans for the facilities where Supplier information systems that process Protected Data are located. Supplier shall verify the established and implemented information security continuity controls at regular intervals.
ii. Data Recovery. Supplier shall design redundant storage and procedures for recovering data in a manner sufficient to reconstruct Protected Data in its original state as found on the last recorded backup provided by the Zipper.

5. Notification and Communication Obligations

a. Notification. Supplier shall without undue delay (i.e., within 48 hours from confirmation) notifyZipper at:Notification to Zipper shall be sent to: privacy@Zipper.com if any of the following events occur:
i. any unmitigated, material security vulnerability, or weakness of which Supplier has actual knowledge in (i) Zipper's systems, or networks, or (ii) Supplier's systems or networks, that has compromised Protected Data;
ii. an Information Security Incident that compromises or is likely to compromise the security of Protected Data and weaken or impair business operations of Zipper;
iii. an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of Protected Data that is Processed, stored, and transmitted using a computer;or
iv. known and willful failure or inability to maintain material compliance with requirements of this ISE and Applicable Laws.b. Cooperation.Supplier shall: (i) respond promptly to any Zipper

reasonable requests for information, cooperation, and assistance, including to a Zipper designated response center.c. Information Security Communication.Except as required by Applicable Laws or by existing applicable contractual obligations, Supplier agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying Zipper, without Zipper's prior written consent. Supplier shall fully cooperate with Zipper and law enforcement authorities concerning any unauthorized access to Zipper's systems or networks, or Protected Data. Such cooperation shall include the retention of all information and data within Supplier's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, Supplier will work with Zipper regarding the timing, content, and recipients of such disclosure. To the extent Supplier was at fault,Supplier will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise.

d. Post-Incident
Supplier shall reasonably cooperate with Zipper in any post-incident investigation, remediation, and communication efforts.

DATA PROTECTION EXHIBIT
ATTACHMENT B1.
SCOPEThis Data Protection Exhibit ("DPE") outlines the terms and conditions with which the Parties must comply with respect to Processing Personal Data and applies to the extent that Supplier Processes or has access to Protected Data in the Performance of its obligations to the Zipper.

2. DEFAULT STANDARDS
a. To the extent that Supplier Processes Special Categories of Data, the security measures referred to in this DPE shall also include, at a minimum (i) routine risk assessments of Supplier's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while during transmission (whether sent by e-mail,fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone). If encryption is not feasible, Supplier shall not store Special Categories of Data on any unencrypted devices unless compensating controls are implemented. Further, Supplier shall protect all Special Categories of Data stored on electronic databases, servers, or other forms of non-mobile devices against all reasonably anticipated forms of compromise by use of the safeguards contained in Attachment A (InformationSecurity Exhibit).

b. In addition to the foregoing, to the extent Supplier receives, processes, transmits or stores anyCardholder Data for or on behalf of Zipper, Supplier represents and warrants that information security procedures, processes, and systems will at all times meet or exceed all applicable information security laws, standards, rules, and requirements related to the collection, storage,Processing, and transmission of payment card information, including those established by applicable governmental regulatory agencies, the Payment Card Industry (the

“PCI”), all applicable networks, and any written standards provided by Zipper’s information security group to Supplier from time to time (all the foregoing collectively the “PCI Compliance Standards”).
c. Where Supplier Processes Protected Health Information (as that term is defined by The HealthInsurance Portability and Accountability Act, or HIPAA), the Business Associate Agreement will be added as Attachment C and will also apply to the Processing of such data. If any of theApplicable Laws are superseded by new or modified Applicable Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Applicable Laws shall be deemed to be incorporated into this DPE, and Supplier will promptly begin complying with such Applicable Laws.d. If this DPE does not specifically address a particular data security or privacy standard or obligation, Supplier will use appropriate, Generally Accepted Practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.
e. Supplier agrees that, in the event of a breach of this DPE, whether Zipper has an adequate remedy in damages, Zipper may be entitled to seek injunctive or equitable relief to immediately cease or prevent the use, Processing, or disclosure of Personal Data not contemplated by theSupplier’s obligations to the Zipper and/or this MDPA and to enforce the terms of this DPE or enforce compliance with all Applicable Laws.
f. Any ambiguity in this DPE shall be resolved to permit Zipper to comply with all Applicable Laws. In the event and to the extent that the Applicable Laws impose stricter obligations on the Supplier than under this DPE, the Applicable Laws shall prevail.

3. CERTIFICATIONS

a. Supplier must maintain the certifications listed in an applicable agreement between the Parties, if any, and Supplier shall recertify such certifications as reasonably required. If there is a material change in the requirements of a required certification or the nature of the PerformanceSupplier is providing, such that Supplier no longer wishes to maintain such certifications, theParties will discuss alternatives and compensating controls in good faith.
b. Prior to Processing Personal Data and at Zipper’s request, Supplier will provide Zipper with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the Processing of Personal Data. Supplier will notify Zipper if Supplier has failed or no longer intends to adhere to such certifications or successor frameworks.

4. DATA PROTECTION AND PRIVACY

a. The Parties agree that, for the Personal Data, Zipper shall be the Data Controller and Supplier shall be the Data Processor.
b. Zipper shall:

i. in its use of the Products and/or Services, comply with Applicable Laws, including maintaining all relevant regulatory registrations and notifications as required under ApplicableLaws;

ii. ensure all instructions given by it to Supplier in respect of Personal Data shall at all times be in accordance with Applicable Laws;
iii. have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Zipper acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Products and/or Services; and
iv. keep the amount of Personal Data provided to Supplier to the minimum necessary for the performance of the Products and/or Services.

c. If Supplier has access to or otherwise Processes Personal Data, then Supplier shall:
i. implement and maintain commercially reasonable and appropriate physical, technical, and organizational security measures described in this DPE (including any appendices or attachments or referenced certifications) designed to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing; and any Information Security Incident;
ii. take reasonable steps designed to ensure the reliability of its staff and that they are subject to a binding written contractual obligation with Supplier to keep the Personal Data confidential (except where disclosure is required in accordance with Applicable Laws, in which case Supplier shall, where practicable and not prohibited by Applicable Laws, notify Zipper of any such requirement before such disclosure) and any other person acting under its supervision who may come into contact with, or otherwise have access to and ProcessPersonal Data; and require that such personnel are aware of their responsibilities under this DPE and any Applicable Laws (or Supplier's own written binding policies that are at least as restrictive as this DPE);
iii. appoint data protection lead(s). Upon request, Supplier will provide the contact details of the appointed person;
iv. assist Zipper as reasonably needed to respond to requests from supervisory authorities, data subjects, customers, or others to provide information (including details of the Services provided by Supplier) related to Supplier's Processing of Personal Data;
v. not transfer Personal Data from the EEA or Switzerland to a jurisdiction which is not an Approved Jurisdiction, unless it first provides Zipper advance notice and an opportunity to object; if Zipper reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate. Where Supplier Processes Personal Data from the EEA or Switzerland on behalf of Zipper,Supplier shall perform such Processing in a manner consistent with the Privacy Shield Principles (see www.commerce.gov/privacyshield) or its successor framework(s) to the extent the Principles are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the Principles, Supplier shall promptly notify Zipper and cease Processing. In such event, Zipper may terminate the applicable Performance of such Processing by written notice within thirty (30) days.
vi. for jurisdictions other than the EEA or Switzerland, not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under ApplicableLaws and it first provides Zipper advance notice and an opportunity to object; if Zipper reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the

objection shall terminate.Where Supplier Processes Personal Data from an APEC Member Economy on behalf ofZipper, Supplier shall perform such Processing in a manner consistent with the APEC CrossBorder Privacy Rules Systems requirements ("CBPRs") (see www.cbprs.org) to the extent the requirements are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the CBPRs, Supplier shall promptlynotify Zipper and cease Processing. In such event, Zipper may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

d. In addition, if Supplier Processes Personal Data in the course of Performance of its obligations to the Zipper, then Supplier shall also:

i. only Process the Personal Data in accordance with Zipper's documented instructions, Appendix 1 of Attachment C and this DPE, but only to the extent that such instructions are consistent with Applicable Laws. If Supplier reasonably believes that Zipper's instructions are inconsistent with Applicable Laws, Supplier will promptly notify Zipper of such;
ii. if required by Applicable Laws, court order, warrant, subpoena, or other legal or judicial process to process Personal Data other than in accordance with Zipper's instructions, notify Zipper of any such requirement before Processing the Personal Data (unless Applicable Laws prohibit such information on important grounds of public interest);
iii. only process or use Personal Data on its systems or facilities to the extent necessary toPerform its obligations solely on behalf of Zipper and only for the purposes contemplatedby the Parties;
iv. where applicable, act as a subprocessor of such Personal Data;
v. maintain reasonably accurate records of the Processing of any Personal Data received from Zipper under the Agreement;
vi. make reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Supplier has the ability to do so;
vii. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed toby separate signed, written agreement;
viii. provide reasonable cooperation and assistance to Zipper in allowing the persons to whom Personal Data relate to have access to their data and to delete or correct such Personal Data if they are demonstrably incorrect (or, if Zipper or Zipper's customer does not agree that they are incorrect, to have recorded the fact that the relevant person considers the data to be incorrect);
ix. provide such assistance as Zipper reasonably requests (either on its own behalf or on behalf of its customers), and Supplier or a Representative is reasonably able to provide, with a view to meeting any applicable filing, approval or similar requirements in relation to Applicable Laws;
x. promptly notify Zipper of any investigation, litigation, arbitrated matter, or other dispute relating to Supplier's information security or privacy practices as it relates to Supplier's Performance of its obligations to Zipper;
xi. provide such reasonable information and assistance as Zipper reasonably requires (taking into account the nature of Processing and the information available to Supplier) to Zipper in ensuring compliance with Zipper's obligations under Applicable Laws with respect to:
A. security of Processing;
B. data protection impact assessments (as such term is defined by ApplicableLaws);

C. prior consultation with a supervisory authority regarding high risk Processing; and
D. notifications to the supervisory authority and/or communications to Data Subjects by Zipper in response to any Information Security Incident; and,

xii. on termination of the MDPA for whatever reason, or upon written request at any time during the Term, Supplier shall cease to Process any Personal Data received from Zipper, and within a reasonable period will, at the request of Zipper: 1) return all Personal Data; or 2) securely and completely destroy or erase (e.g. using a standard such as US Department of Defense 5220.22-M, NIST 800-53, or British HMG InfoSec Standard 5, Enhanced Standard) all Personal Data in its possession or control unless such return or destruction is not feasible or continued retention and Processing is required by Applicable Laws. At Zipper's request, Supplier shall give Zipper a certificate signed by one of its senior managers, confirming that it has fully complied with this Clause.

5. STANDARD CONTRACTUAL CLAUSES FOR THE PROCESSING OF PERSONAL DATA

If, and only with Zipper's prior consent, Supplier Processes Personal Data from the EEA or Switzerland or in a jurisdiction that is not an Approved Jurisdiction, the Parties shall confirm there is a legally approved mechanism in place to allow for the international data transfer. If Supplier intends to rely on Standard Contractual Clauses (rather than another permissible transfer mechanism), the following additional terms will apply to Supplier and Supplier's subprocessors and/or Affiliates who may be Performing on behalf of the Supplier:

a. The Standard Contractual Clauses set forth in Attachment D will apply. If such Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the Parties shall promptly enter into the new or modified Standard Contractual Clauses, as necessary.
b. If Supplier subcontracts any Processing of Personal Data (only as expressly allowed by an applicable agreement between the Parties and Applicable Laws), Supplier will:
i. Notify Zipper in advance of such Processing and provide Zipper an opportunity to object prior to Processing; and
ii. Require that Supplier's subprocessors have entered into written agreements with Supplier in which the subprocessors agree to abide by terms consistent with the applicable portions of the Standard Contractual Clauses with respect to such Personal Data.

c. If necessary to comply with Applicable Laws, and where reasonably requested by Zipper on behalf of its customers, Supplier shall enter into the Standard Contractual Clauses directly with Zipper's customers.

6. SUBPROCESSING

a. Supplier shall have a documented security program and policies that provide (i) guidance to its subprocessors with respect to ensuring the security, confidentiality, integrity, and availability

of personal data and systems maintained or processed by Supplier; and (ii) express instructions regarding the steps to take in the event of a compromise or other anomalous event.
b. Supplier shall not subcontract its obligations under this DPE to another person or entity, in whole or in part, without providing Zipper with advance notice and an opportunity to object; if Zipper reasonably objects to the proposed subcontracting the applicable Performance that is the subject matter of the objection shall terminate.
c. Supplier will execute a written agreement with such approved subprocessors containing terms at least as protective as this DPE and the applicable Exhibits (provided that Supplier shall not be entitled to permit the subprocessor to further subcontract or otherwise delegate all or any part of the subprocessor's Processing without Supplier's prior notice and opportunity to object) and designating Zipper as a third party beneficiary with rights to enforce such terms either by contract or operation of law. Further, if privity of contract is required by Applicable Laws, Supplier shall procure that any such subprocessors cooperates and enters into any necessary additional agreements directly with Zipper.
d. Supplier shall be liable and accountable for the acts or omissions of Representatives to the same extent it is liable and accountable for its own actions or omissions under this DPE.
e. Zipper acknowledges and expressly agrees that (a) Supplier's Affiliates may be retained as subprocessors, and (b) Receiving Party and Supplier's Affiliates respectively may engage third party subprocessors in the course of Performance. Supplier shall make available to Zipper a current list of subprocessors for the respective Services with the identities of those subprocessors ("Subprocessor List") upon Zipper's reasonable request.

7. RIGHTS OF DATA SUBJECTS

a. Data Subject Requests. Supplier shall, to the extent legally permitted, promptly notify Zipper if it receives a request from a Data Subject for access to, correction, portability, or deletion of suchData Subject's Personal Data. Unless required by Applicable Laws, Supplier shall not respond to any such Data Subject request without Zipper's prior written consent except to confirm that the request relates to Zipper. In addition Supplier shall provide such information and cooperation and take such action as the Zipper reasonably requests in relation to a Data Subject request.
b. Complaints or Notices related to Personal Data. In the event Supplier receives any official complaint, notice, or communication that relates to Supplier's Processing of Personal Data or eitherParty's compliance with Applicable Laws in connection with Personal Data, to the extent legally permitted, Supplier shall promptly notify Zipper and, to the extent applicable, Supplier shall provide Zipper with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Zipper shall be responsible for any reasonable costs arising from Supplier's provision of such assistance.

ATTACHMENT C BUSINESS ASSOCIATE AGREEMENT

For purposes of this Business Associate Agreement Attachment, the Supplier shall be hereinafter referred to as "Business Associate".

RECITALS WHEREAS, Subtitle F of the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, as amended by the American Recovery and Reinvestment Act of 2009, Public Law No. 111-005, Part I, Title XIII, Subpart D, Sections 13401-13409, (the “HITECH Act”), (collectively, “HIPAA”) provides that Supplier comply with standards to protect the security, confidentiality and integrity of health information; and WHEREAS, the Department of Health and Human Services has issued regulations under HIPAA (the “HIPAA Regulations”), including the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, sub-parts A and E, as amended by the HITECH Act (the “Privacy Rule”) and the Standards for Security of Electronic Protected Health Information, 45 CFR Parts 160, 162 and 164, as amended by the HITECH Act (the “Security Rule”) (collectively, the “Privacy and Security Rules”); and WHEREAS, Sections 164.502(e) and 164.504(e) of the Privacy and Security Rules set forth standards and requirements for Zipper to enter into written agreements with certain business associates that will have access to Protected Health Information (as defined below); and WHEREAS, Business Associate will provide services under the Agreement as a subcontractor to Zipper on behalf of a Covered Entity (as defined in the Privacy and Security Rules).

NOW THEREFORE, in consideration of the mutual promises below, the Parties agree as follows:

1. Definitions
1.1. “Breach” shall have the meaning given to such term in 45 CFR Section 164.402.
1.2. “Designated Record Set” shall have the meaning given to such term under the Privacy Rule at 45 CFR Section 164.501.
1.3. “Electronic Protected Health Information” or “Electronic PHI” shall mean Protected Health Information which is transmitted by Electronic Media (as defined in the Privacy and Security Rules) or maintained in Electronic Media.
1.4. "Individual" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).
1.5. “Protected Health Information” or “PHI” shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103, limited to the information created or received by Business Associate from or on behalf of Zipper. “Protected Health Information” includes, without limitation, “Electronic Protected Health Information”.
1.6. “Required by Law” shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103.
1.7. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.
1.8. “Security Incident” shall have the meaning given to such term under the Security Rule at 45 CFR Section 164.304.

2. Permitted Uses and Disclosures of PHI. Business Associate agrees not to use or further disclose PHI other than as permitted or required by this Attachment or as otherwise Required

By Law. In connection with the foregoing and except as otherwise limited in this Attachment, Business Associate may:

2.1. Use or disclose PHI to perform functions, activities or services for, or on behalf of, Zipper that are necessary to Perform under the Agreement or applicable SOW, provided that such use or disclosure would not violate the Privacy and Security Rules if done by Zipper;
2.2. Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; and
2.3. Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and that the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Responsibilities of Business Associate.
3.1. Appropriate Safeguards. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the Attachment. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule. In furtherance of compliance with such requirements, Business Associate shall:
3.1.1. maintain an information security program that meets or exceeds the level required by the HIPAA Security Rule;
3.1.2. maintain policies and procedures for Business Associate's organization, consistent with theHIPAA Privacy and Security Rules and must identify an individual within the Business Associate's organization who is responsible for enforcement and oversight of such privacy and security policies and procedures;
3.1.3. ensure that any and all employees of Business Associate that handle or access PHI must undergo ongoing training regarding the safeguarding of PHI;
3.1.4. ensure that any and all third parties that access Covered Entity's confidential data or PHI with whom Business Associate contracts with or relies upon for the provision of services also maintain a framework for compliance with the HIPAA Privacy and Security Rules;
3.1.5. implement a contingency plan for responding to emergencies and/or disruptions to business that in any way affect the use, access, disclosure or other handling of Covered Entity's data and PHI;
3.1.6. maintain and exercise a plan to respond to internal and external security threats and violations, including an incident response plan;
3.1.7. maintain policies and procedures that specifically address how security breaches that are identified will be addressed;
3.1.8. maintain technology policies and procedures that provide reasonable safeguards for the protection of PHI on hardware and software utilized by Business Associate;

3.1.9. ensure that for the electronic transmission of PHI is encrypted meeting at least the minimum standards required by Zipper's data security policies and applicable National Institute of Standards and Technology guidelines.

3.2. Security Survey. During the term of this Attachment, Business Associate may be asked to complete a security survey and/or attestation document designed to assist Zipper in understanding and documenting Business Associate's security procedures and compliance with the requirements contained herein. Business Associate's failure to complete either of these documents within the reasonable timeframe specified by Zipper shall constitute a material breach of the Agreement.
3.3. Additional Information. Business Associate shall provide Zipper with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Covered Entity's PHI, as Zipper may from time to time request. Failure of Business Associate to complete or to respond to Zipper's request for information within the reasonable timeframe specified by Zipper shall constitute a material breach of the Agreement. If Zipper has reasonable concern regarding compliance with the terms of this Attachment or the occurrence of a breach, Zipper will be granted access to facilities in order to review policies, procedures and controls relating to the compliance with the terms of this Attachment.
3.4. Reporting of Improper Use or Disclosure. Business Associate shall promptly report to Zipper any use or disclosure of PHI not provided for by the Attachment of which it becomes aware, including breaches of Unsecured Protected Health Information (as defined in the Privacy and Security Rules). In addition, Business Associate shall promptly report to Zipper any Security Incident. If Zipper determines that such use or disclosure may constitute a Breach of Unsecured Protected Health Information, Business Associate agrees to provide Zipper written notification of the Breach that includes the following information within three (3) days:

(1) a brief description of the incident, including the date of the Breach and the date of the discovery of the Breach;
(2) the identification of each individual whose Unsecured PHI was breached;
(3) a description of the types of Unsecured PHI that were involved in the Breach;
(4) any steps individuals should take to protect themselves from potential harm resulting from the Breach; and
(5) a brief description of actions that Business Associate is undertaking to investigate the Breach, to mitigate harm to individuals, and to protect against any further breaches.

3.5. Business Associate's Agents. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides any PHI received from Zipper agrees to the same restrictions and conditions that apply through this Attachment to Business Associate with respect to such PHI.
3.6. Access to PHI. At the request of Zipper, and in the time and manner designated by Zipper, Business Associate shall make available PHI in a Designated Record set to Zipper as necessary to meet the requirements under 45 CFR Section 164.524.

3.7. Amendment of PHI. At the request of Zipper, and in the time and manner designated by Zipper, Business Associate shall make any amendment(s) to PHI maintained in a Designated Record Set pursuant to 45 CFR Section 164.526.
3.8. Documentation of Disclosures. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Zipper to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.
3.9. Accounting of Disclosures. Business Associate agrees to provide to Zipper, in the reasonable time and manner designated by Zipper, information collected in accordance with Section 4(f) of this Attachment, to permit Zipper to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.
3.10. Governmental Access to Records. Business Associate shall make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Zipper available to the Secretary for purposes of the Secretary determining Zipper's compliance with the Privacy and Security Rules.

4. Responsibilities of Zipper. In addition to any other obligations set forth in this Attachment, Zipper shall:
4.1. provide to Business Associate only the minimum PHI necessary to accomplish the services;
4.2. implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule; and
4.3. obtain any consent or authorization that may be required by applicable or federal or state laws and regulations prior to furnishing PHI to Business Associate.

5. Term and Termination. The term of this Attachment shall commence as of the Effective Date and continue coterminous with the Agreement unless otherwise terminated as set forth herein. Upon Zipper's knowledge of a material breach by Business Associate of this Attachment, Zipper shall either
(i) provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Zipper, or
(ii) immediately terminate this Attachment if cure is not possible. Upon termination of this Attachment for any reason, Business Associate shall return or destroy all PHI received from Zipper, or created or received by Business Associate on behalf of Zipper, and shall retain no copies of PHI. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Zipper notification of the conditions that make return or destruction infeasible. If Business Associate determines that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this

Attachment to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

6. Regulatory References. A reference in this Attachment to a section in the Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.

7. No Agency Relationship. The Parties agree that each individual party shall maintain its own independent HIPAA and HITECH Act compliance obligations. The Parties will be providing their services as separate legal entities and independent contractors. The Parties expressly agree that no agency relationship is created by this Attachment or the underlying Agreement with regard to the individual parties' HIPAA obligations. Each party certifies that
(1) Zipper shall not have the right or authority to control Business Associate's conduct in the performance of services or in the performance of HIPAA obligations;
(2) Zipper shall not have the authority to direct the daily performance of services by Business Associate; and
(3) Zipper shall not have the right to give interim instruction to Business Associate regarding the performance of services.

8. Interpretation. Any ambiguity in this Attachment shall be resolved to permit Zipper to comply with the Privacy and Security Rules.

ATTACHMENT D

Standard Contractual ClausesFor the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (These can be located in their original text on the European Commission website here:
http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).
For purposes of this Attachment D: any reference to "data exporter" means Zipper, acting as data exporter on behalf of its EEA or Swiss customer(s) where applicable, and any reference to "data importer" means Supplier each a "party"; together "the parties".The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.
Clause 1 Definitions For the purposes of the Clauses:
(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Clause 2 Details of the transfer The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
Clause 3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the data exporter The data exporter agrees and warrants:
(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the

Member State where the data exporter is established) and does not violate the relevant provisions of that State;
(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
(e) that it will ensure compliance with the security measures;
(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and (j) that it will ensure compliance with Clause 4(a) to (i).Clause 5Obligations of the data importer The data importer agrees and warrants:(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract; (c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;(d) that it will promptly notify the data exporter about: (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition

under criminal law to preserve the confidentiality of a law enforcement investigation, (ii) any accidental or unauthorised access, and (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred; (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 Liability 1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction
1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;(b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 Cooperation with supervisory authorities
1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 Governing Law The Clauses shall be governed by the law of the Member State in which the data controller is established.

Clause 10 Variation of the contract
The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 Subprocessing
1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to

exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data controller is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 Obligation after the termination of personal data processing services
1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.APPENDIX 1 TO ATTACHMENT DTHE STANDARD CONTRACTUAL CLAUSES

This Appendix 1 forms part of the Clauses.Data exporterThe data exporter is Zipper, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Zipper and its customer(s).

Data importerThe data importer is Supplier. Activities relevant to the transfer include the performance of services for Zipper and customers. Data subjects
The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of customers, and other individuals whose personal data is processed by or on behalf of Zipper or Zipper’s customers and delivered as part of the Services. Categories of dataThe personal data transferred may concern the following categories of data: Personal Data related directly or indirectly to the delivery of services or Performance, including online and offline customer, prospect, partner, and Supplier data, and personal data provided by customers in connection with the resolution of support requests.Special categories of dataThe personal data transferred may concern the following special categories of data: Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, and data concerning health or sex life, and data relating to offenses, criminal convictions or security measures.

Processing operations The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Zipper and customers: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to customers, including services offered by means of the products and solutions described by Supplier, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.

APPENDIX 2 TO ATTACHMENT DTHE STANDARD CONTRACTUAL CLAUSES Appendix 2 to Attachment D, the Standard Contractual Clauses, is the Information Security Exhibit (“ISE”) located at Attachment A.

ATTACHMENT E

GLOSSARY OF TERMS

All capitalized terms not defined in this Glossary have the meanings set forth elsewhere in the MDPA.

a. “Administrative Data” means data related to employees or representatives of Zipper that is collected and used by Supplier in order to administer or manage Supplier’s Performance, or the Zipper’s account, for Supplier’s own business purposes. Administrative Data may include Personal Data and information about the contractual commitments between Zipper and Supplier, whether collected at the time of the initial registration or thereafter in connection with the delivery, management or Performance. Administrative Data is Protected Data.

b. "Affiliates" means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, for so long as such control exists. In the case of companies and corporations, "control" and "controlled" mean beneficial ownership of more than fifty percent (50%) of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" mean the ability to directly or indirectly control the management and/or business of the legal entity.

c. “APEC” means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.

d. “APEC Member Economy” means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand,United States, and Vietnam.

e. “Applicable Laws” means any applicable country, federal, state, and local law, ordinances, statute, by-law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), compulsory guidance of a regulatory body with authority over the applicable Party, rule of court or directives, binding court decision or precedent, or delegated or

subordinate legislation, each of the above as may be amended from time to time. Parties will comply with all laws, all licenses, permits and approvals required by any government or authority, and shall comply with all applicable laws, rules, policies and procedures. For avoidance of doubt, Applicable Laws includes data protection and privacy laws of each jurisdiction where a Zipper entity that is legally responsible for such Personal Data is established and those of each jurisdiction where such Personal Data is collected or otherwise processed.

f. “Approved Jurisdiction” means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.g. “Business Associate Agreement” means the specific terms and conditions that apply when the Supplier Processes Protected Health Information.

h. “Cardholder Data” is a category of Sensitive Personal Data and includes a cardholder's name, full account number, expiration date, and the three-digit or four-digit security number printed on thefront or back of a payment card. Cardholder Data is Protected Data.

i. “Confidential Information” means any confidential information or materials relating to the business, products, customers or employees of the Zipper and includes, without limitation, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software source documents, data, customer lists, financial information, pricing, product development, sales and marketing plans or information that the Supplier knows or has reason to know is confidential, proprietary or trade secret information obtained by Supplier from the Zipper or at the request or direction of the Zipper in the course of Performing: (i) that has been marked as confidential; (ii) whose confidential nature has been made known by the Zipper to the Supplier; or (iii) that due to their character and nature, a reasonable person under like circumstances would treat as confidential.

j. “Customer Data” means all data (including text, audio, video, or image files) that is either provided by a customer in connection with the customer’s use of products or services, or data developed at the specific request of a customer pursuant to a statement of work or contract. Customer Data doesnot include Administrative Data, Financing Data, Support Data or Telemetry Data.

k. “Data Subject” means the individual to whom Personal Data relates.

l. “Zipper” means that party making available Protected Data (whether confidential or not) to the other party.m. “EEA” or “European Economic Area” means those countries that are members of European Free Trade Association (“EFTA”), and the then-current, post-accession member states of the EuropeanUnion.

n. “Electronic Protected Health Information” or “Electronic PHI” shall have the meaning given to such term as set forth in the Business Associate Agreement.

o. “Financing Data” means information related to Zipper’s financial health that Zipper provides to Supplier in connection with the Agreement. Financing Data is Protected Data.

p. “Generally Accepted Practices” refer to the levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-current accepted industry standards of first-tier providers of the tasks contemplated in Performance of the Agreement.

q. “Information Security Incident” means a successful or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.
r. “Performance” means any acts by either Party in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service (“SaaS”), cloud platforms or hosted services. “Perform,” “Performs,” and “Performing” shall be construed accordingly.
s. “Personal Data” means any information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person. Personal Data shall be considered Confidential Information regardless of the source. Personal Data is Protected Data.
t. “Process” means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. “Processes” and “Processing” shall be construed accordingly.
u. “Product” means Supplier hardware and software products.
v. “Protected Data” means Administrative Data, Confidential Information, Customer Data, Financing Data, Cardholder Data, Support Data, Telemetry Data, and all Personal Data.
w. “Protected Health Information” or “PHI” shall have the meaning given to such term as set forth in the Business Associate Agreement and is a category of Personal Data. “Protected Health Information” includes “Electronic Protected Health Information” or “ePHI”.
x. “Supplier” means the Party receiving Protected Data.
y. “Representatives” means either Party and its Affiliates’ officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.
z. “Sensitive Personal Data” or “Special Categories of Data” means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by Applicable Laws and include: information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, precise geolocation over time, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Zipper may require additional privacy responsibilities when dealing with such Personal Data, which will be appended to the Agreement or a statement of work, as applicable.
aa. “Service” means a service offering from Supplier described in an applicable service or offer description, statement of work, or purchase order listed selected by Zipper.
bb. “Support Data” means information that Supplier collects when Zipper submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files. Support Data is Protected Data.

cc. “Telemetry Data” means information generated by instrumentation and logging systems created through the use and operation of the products and/or services. Telemetry Data is Protected Data.