PURCHASE ORDER TERMS

If FIS and Provider (as defined below) have executed a written agreement which expressly relates to the Purchase Order, such terms and conditions shall apply to the Purchase Order. Otherwise, the following terms and conditions ("**Purchase Order Terms**") shall govern the Purchase Order and shall be deemed incorporated to it, and each Purchase Order, together with these Purchase Order Terms, shall form a separate agreement ("**Agreement**"), by and between FIS and Provider. In the event of any conflict between the Purchase Order and these Purchase Order Terms, the latter shall prevail.

DEFINITIONS

"Affiliate" is, with respect to a party, an entity which, directly or indirectly, is controlled by or is under common control with that party, where "control" of the party or other entity is the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the party or other entity, whether through record or beneficial ownership of voting securities, by contract or otherwise.

"**Change in Control**" of Provider is any event or series of events by which (i) any person, entity or group of persons or entities acquires control of Provider, where "control" is possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of Provider, whether through record or beneficial ownership of voting securities, by contract or otherwise, or (ii) if Provider is a corporation, limited liability company or other entity having a board of directors or other group of individuals having similar functions, during any period of twelve (12) consecutive months commencing before or after the date hereof, individuals who at the beginning of such twelve-month period were members of Provider's board of directors or other such group cease for any reason to constitute a majority of the members.

"**Claim**" is any action, litigation, or claim for which a party is subject to an indemnification obligation under the Purchase Order.

"Client" is any current or prospective client or other customer of FIS or an FIS Affiliate.

"Contractor", with respect to a party, is any individual (other than the party or an employee of the party), corporation or other entity providing services to or on behalf of the party, including any direct or indirect independent contractor to the party.

"**Destructive Element**" is any computer code or other technological device which (i) is intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of a software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"), (ii) would disable a Product or Service or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices), (iii) would permit Provider, any Provider Personnel or any licensor or Contractor to Provider to access a Product or Service to cause such disablement or impairment (sometimes referred to as "traps," "access codes" or "trap door" devices), or (iv) contains any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause a Product or Service or any other software, firmware, hardware, computer system or network to cease functioning or damage or corrupt data, storage media, programs, equipment or communications or otherwise interfere with the operations of FIS, Clients or their customers.

"**Documentation**" means the user manuals, training materials, specifications, release notes, and other written documentation, as applicable, made available by Provider from time to time to FIS in connection with and/or related to software.

"FIS" is (unless otherwise specified on Purchase Orders outside the United States) **FIDELITY INFORMATION SERVICES, LLC**, an Arkansas limited liability company located at 601 Riverside Avenue, Jacksonville, Florida 32204. Purchase Orders outside the United States may specify an Affiliate of Fidelity Information Services, LLC, in which "FIS" shall refer to such specified Affiliate.

"**Force Majeure Event**" is an event that prevents a party's performance of an obligation under the Purchase Order and is beyond the reasonable control of the party, such as a natural disaster, strike, riot, earthquake, epidemic, terrorist action, war, fire, flood, unavailability of communications or electrical service provided by a third party, or governmental regulations imposed after the fact.

"**GDPR**" means, as appropriate and as amended from time to time: (i) the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**").

"Good Industry Practice" is the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances.

"Guidelines" are the standards and guidelines established pursuant to (i) the Gramm-Leach-Bliley Act of 1999 or a state law equivalent, relating to the protection of NPI, (ii) the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent, relating to the protection of PHI, (iii) other relevant privacy Laws, or (iv) PCI DSS, relating to Payment Card Data.

"Information Breach" is any actual or attempted unauthorized intrusion or other breach to the network, systems, or security of or under the management or control of Provider affecting FIS data, including any actual or attempted access to or use, possession or release of NPI, PHI, Personal Data, Payment Card Data or other FIS Confidential Information.

"Law" is applicable laws collectively, including statutes, codes, rules, regulations, ordinances and orders of governmental authorities.

"**NPI**" is "nonpublic personal information" protected under the Gramm-Leach-Bliley Act of 1999 or a state law equivalent.

"**Payment Card Data**" is cardholder data protected under the Payment Card Industry Data Security Standard (PCI DSS).

"**Personal Data**" shall have the same meaning as in the GDPR.

"**PHI**" is "protected health information" protected under the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent.

"**Privacy Regulations**" are the standards, guidelines and other regulations established by various federal or state regulatory agencies to protect the privacy and security of customer or patient information held by financial institutions, medical service providers and other entities.

"Products" are the materials, goods, and anything else, excluding Services, to be sold or to be provided by Provider as specified in the Purchase Order and/or any part thereof.

"Provider" is any person or company or other entity providing Products and/or Services to FIS under the Purchase Order.

"Provider Personnel" are individuals who are assigned to perform a Service, including employees of Provider or its Affiliates, employees of any Contractor to Provider, and if Provider is an individual, Provider or any Contractor to Provider.

"Purchase Order" means the document in a form provided by FIS (which may be electronic or otherwise incorporated into a purchasing system) which describes the Products and/or Services to be provided by Provider to FIS and the fees, payment terms, delivery specification and other similar provisions applicable thereto.

"Services" are services provided under the Purchase Order for data processing, software hosting, software as a service, a knowledge or information service, provision of work or workers on an outsourced basis, production management, customization or other custom development, training and support, and various other matters as requested by FIS and as more particularly described in the Purchase Order.

"Term" is the time period during which the Purchase Order is effective.

PART 1. PURCHASE AND SALE, TERM, PACKING, DELIVERY, INSPECTION, ACCEPTANCE.

a. PURCHASE AND SALE. Provider agrees to provide, and FIS agrees to purchase the Products and/or Services set forth on the Purchase Order in accordance with the terms of the Purchase Order and the provisions herein. The Products and/or Services are provided for the benefit of FIS and its Affiliates globally.

b. TERM. The Purchase Order may set forth the Term during which the Purchase Order is effective. If no such Term is specified, then the Purchase Order become effective on execution and shall expire upon the full performance of both parties.

c. EXPIRATION AND RENEWAL.

(1) If the Term is set forth on the Purchase Order, Provider will notify FIS of each date the Term will expire, within no more than one hundred eighty (180) days nor less than ninety (90) days before that date.

(2) If the Purchase Order provides for automatic renewal or extension of the Term or for automatic renewal or extension of any Products or Services, lease or license, or if the Purchase Order provides for renewal or extension at the option of FIS, Provider will notify FIS of the date by which FIS must give any prior written notice required to prevent or elect renewal, as the case may be, within no more than ninety (90) days nor less than forty-five (45) days before that date. Provider will include in any such notification the requirements for a timely notice by FIS.

(3) During the period following any notification by Provider under paragraph (1) or (2) above, Provider and FIS will mutually discuss the basis upon which they may wish to renew or extend the Term, Products, Services, lease or license, as applicable. However, FIS' right to prevent automatic renewal or extension or elect a renewal or extension, as the case may be, will be unconditional, subject only to FIS giving timely notice of nonrenewal or renewal.

d. TERMINATION. FIS may terminate the Purchase Order, or any Products, Services, lease or license thereunder, without penalty, (i) at any time upon giving Provider no less than thirty (30) days prior written notice of its intent to do so or (ii) in the event of a Change in Control of Provider, immediately upon written notice to Provider. In the event of any termination by FIS pursuant to this Section d, FIS will be obligated to pay for the Products properly delivered and accepted and the Services successfully completed by Provider through the effective date of such termination.

e. PACKING AND DELIVERY. Unless stated otherwise, for Products that are not delivered electronically, Provider will pack all Products in a manner that is: (i) in keeping with good commercial practices, (ii) acceptable to common carriers for shipment at the lowest rate for the particular Products, (iii) in accordance with I.C.C. regulations and (iv) adequate to ensure safe arrival of the Products at the specified destination. Provider will mark all containers with the applicable lifting, handling and shipping information that includes Purchase order numbers, Provider's part number, manufacturer's part number, part serial numbers, the number of cartons, and any other unique markings that may be required by the FIS from time to time. Unless otherwise specified on the Purchase Order, the Products ordered hereunder will be delivered F.O.B. FIS' "Ship To" location. Title and risk of loss or damage to all Products will pass to FIS upon FIS' actual receipt of the Products at the specified place of delivery. Provider will also bear the risk of loss as to any Products rejected by FIS, except that FIS will be responsible for any damage to rejected or unaccepted Products caused by the willful misconduct of its employees acting within the scope of their employment.

f. INSPECTION AND ACCEPTANCE.

(1) The following shall apply to Products: At FIS' request, Provider shall ensure that FIS, or any third party appointed by FIS, has the opportunity to inspect and/or test (or witness any testing of) the Products at any time prior to or within a reasonable time following delivery, and Provider shall furnish all reasonable assistance.

(2) The following shall apply to Services: FIS may test the Services within a reasonable period following delivery to ensure they conform to the agreed specifications, and Provider shall furnish all reasonable assistance.

Such inspection or testing, including the witnessing thereof, shall not relieve Provider from any of its responsibilities and liabilities under the Purchase Order. If a Product or Service is defective (which in the case of the Services, means they fail to conform to the agreed specifications), or does not conform to the requirements of the Purchase Order, FIS will have the right to reject it, to require its correction or reperformance, or to accept it with an adjustment in price. Any Products or Services that have been rejected or require correction/reperformance must be replaced or corrected by and at the sole expense of the Provider promptly after notice. Should Provider fail to promptly replace or correct or reperform any defective item, FIS

may (i) replace or correct or reperform such item and charge to Provider the cost occasioned thereby, (ii) without further notice, cancel the Purchase Order for default and receive a full refund of the price paid, or (iii) require a corresponding reduction in price.

PART 2. SAFETY AND SECURITY.

a. SAFETY AND SECURITY ON PREMISES. All Provider Personnel must comply with all FIS postings and notices regarding safety and security when on the premises of FIS, and with the postings and notices of Clients or their customers when on their premises. Provider Personnel must not carry weapons or ammunition onto the premises of FIS, Clients or their customers and must not use or carry weapons or ammunition while attending FIS-sponsored events.

b. ACCESS PRIVILEGES AND RESTRICTIONS. If Provider Personnel will receive access credentials for FIS' facilities, applications, systems or servers, those of its Affiliates or those of any Clients or any of their customers, the following provisions will also apply:

(1) Provider will require all Provider Personnel that will be issued access credentials to submit to FIS' then current access requirements.

(2) Provider will promptly, but in any event within twenty-four (24) hours, (i) confiscate each such access credential from Provider Personnel when the Provider Personnel's need to have such access in order for the Services to be performed or Products to be provided is discontinued and (ii) notify FIS of any change in the status (including any such suspension, termination or discontinuation) of Provider Personnel for whom such a device or access credential has been requested or to whom such a device or access credential has been provided.

(3) Provider will not request that such an access credential be provided, or provide such an access credential, to any individual who will not be directly engaged by or at the request of FIS to provide the Services or the Products.

(4) FIS reserves the right to deny any access credential request or terminate any access credential that has been provided. Provider will notify FIS within twenty-four (24) hours of any changes to the Provider Personnel for whom such an access credential has been requested or to whom such an access credential has been provided.

(5) Provider will not permit any such access credential to be used by more than one individual.

c. INFORMATION SECURITY AND INTERNAL CONTROLS. Provider shall comply with FIS' information security requirements set forth in **Appendix A**, which appendix is attached hereto and incorporated herein by this reference.

d. BACKGROUND CHECKS. Provider will perform the background check, as described herein, and also timely cooperate in good faith with FIS' performance of a background check, as described herein, for each individual who is performing any Services under the Agreement and has access to the facilities, records or data of FIS, any Affiliate, any Client or any customer of a Client. Where permitted by applicable Law, the background check will consist of, at a minimum, verification of the highest level of education completed, verification of employment for the past six (6) years, social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and export denial lists. In addition, to the extent permitted by Law, the background check will include an 8-panel drug test (test to exclude Marijuana/THC) and criminal record search. For the drug test, all specimens will be tested at a Department of Health and Human Services/Substance Abuse Mental Health Services Administration certified lab, and the screening service will include confirmation of all positive test results. The criminal record search will include, to the maximum extent permitted by Law, a federal, state and county check, and a National Criminal File check, for felony and misdemeanor convictions for the last ten (10) years in all locations where the individual has resided for the last ten (10) years. Provider will comply with all applicable Laws related to the background check, including required notices and applicable consents. In addition, Provider will require the individual to report any criminal convictions. Provider will not assign anyone to perform Services for FIS who has tested positive for drugs or whose background check findings do not meet the standards established by Provider in accordance with all applicable Laws, including if there is a conviction or referral to a pretrial diversion program for a crime that is related to his or her duties.

Provider acknowledges that under the banking Laws, an individual may not participate, directly or indirectly, in any manner in the conduct of the affairs of any insured depository institution without regulatory consent if he or she has a conviction, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution, of a crime involving dishonesty, breach of trust or money laundering, including any crime concerning the illegal manufacture, sale, distribution of or trafficking in controlled substances, unless the crime meets certain criteria for treating the crime as de minimis. The background check must be completed before assignment of an individual and periodically thereafter. FIS also reserves the right to request that Provider provide an attestation confirming a background check as required by this provision has been completed and no disqualifying information has been identified on an annual basis during the Term of an Engagement. Upon five (5) Business Days' prior written notice, FIS may verify Provider's compliance with this Section. Such verification will be conducted in a manner that minimizes disruption to Provider's business. FIS may use an independent auditor to assist with such verification, provided that FIS has a written confidentiality agreement in place with such independent auditor. FIS will notify Provider in writing if any such verification indicates that Provider is not in compliance with this Section and Provider will promptly remediate any issues of non-compliance discovered by FIS as part of such verification. Further, if requested by FIS for any reason, Provider shall immediately remove a Provider Personnel from the provision of the Products or Services.

PART 3. SAFEGUARDING OF INFORMATION.

a. PROTECTION OF CONFIDENTIAL INFORMATION. Each party must protect the other's Confidential Information with the same degree of care used to protect its own Confidential Information, but in no event may either party use less than a reasonable standard of care be in connection with the preservation of the other's Confidential Information. FIS designates as its Confidential Information (i) the Purchase Order, (ii) any information obtained from or related to any Client of FIS including FIS Client business strategy, direction and contract information, (iii) any NPI, PHI, or Payment Card Data (iv) FIS' employee records (name, address, phone number, salary, taxpayer or government identification number, date of birth, health records, bank account information, labor party), (v) any business strategies and directions, operating or marketing plans, intellectual capital or trade secrets, (vi) memos or other documents or communications pertaining to pending FIS litigation or contracts (including the Purchase Order), (vii) any information disclosed by FIS that is designated as "confidential" at or prior to disclosure, (viii) other FIS data or information which is not generally known, including business information, specifications, research, software, trade secrets, discoveries, ideas, know-how, designs, drawings, flow charts, data, computer programs, marketing plans, budget figures, and other financial and business information, and (ix) information of the kind described by any of the foregoing categories that is of or disclosed by a Client, an FIS Affiliate, or a customer of a Client. Provider will (A) restrict the use and disclosure of the FIS' Confidential Information to its Provider Personnel and do so solely on a "need to know" basis in connection with Provider's obligations to provide Products or to perform Services in accordance with the Purchase Order, (B) ensure Provider Personnel who receive or have access to FIS Confidential Information are bound by confidentiality obligations at least as restrictive and as protective of the FIS Confidential Information as the provisions of this Section, (C) require its Provider Personnel to protect and restrict the use of the FIS' Confidential Information, (D) establish procedural, physical and electronic safeguards, designed to prevent the compromise or unauthorized disclosure of FIS Confidential Information and to achieve the objectives of the Guidelines (if applicable), (E) promptly investigate any security breach to determine whether such incident has resulted or is likely to result in misuse or unauthorized possession or disclosure of FIS Confidential Information and (F) not use or disclose FIS' Confidential Information except in accordance with the Purchase Order.

(1) In providing any notice of an Information Breach, Provider will use commercially reasonable efforts to (i) provide notice to one or more FIS managers generally responsible for security matters relating to the FIS Confidential Information affected by the Information Breach, within twenty-four (24) hours of discovering the Information Breach, and (ii) keep FIS informed as to the actual and anticipated effects of the Information Breach and the corrective actions taken or to be taken in response to the Information Breach. In addition, if the Information Breach results or is likely to result in misuse of NPI, PHI or Payment Card Data, Provider will (A) notify FIS as soon as possible and reasonably cooperate with FIS in its efforts to notify affected Clients and their customers and to mitigate the actual or potential harm resulting from the Information Breach and (B) reimburse FIS for its reasonable costs in notifying Clients or their customers of the

Information Breach and making available to them any credit monitoring services and for any other costs FIS reasonably incurs with respect to the Information Breach.

(2) Confidential Information will remain the property of the party from or through whom it was provided. Except for NPI, PHI, Payment Card Data, or other information protected by the Guidelines, the parties' respective confidentiality obligations under the Agreement do not apply to any information that: (i) was previously known by the party; (ii) is a matter of public knowledge; (iii) was or is independently developed by the party; (iv) is released for disclosure with written consent of the party; or (v) is received from a third party to whom it was disclosed without restriction.

(3) Each party may disclose information notwithstanding its confidentiality obligations under the Purchase Order to the extent required (i) by Law, (ii) in connection with the tax treatment or tax structure of the Purchase Order; or (iii) in response to a valid order of a U.S. court or other governmental body, provided that the party provides the other party with written notice and the other party is afforded a reasonable opportunity to obtain a protective order with respect to the disclosure.

(4) Upon termination of the Purchase Order, Provider will destroy all FIS Confidential Information in a manner designed to preserve its confidentiality, or, at FIS' written request, return it to FIS. Upon FIS' written request, Provider shall, at FIS' choice, delete or return all Personal Data Processed on behalf of FIS to FIS after the end of the provision of Services relating to Processing, subject to Provider retaining any copies required by applicable EU member state law.

(5) FIS will have and retain all right, title and interest in all of FIS' Confidential Information, whether possessed by FIS prior to, or acquired or refined by FIS (either independently or in concert with Provider) during the Term.

(6) Provider will not, without the prior written consent of FIS, (i) provide the Products or Services or access, store or process any of FIS' Confidential Information outside the United States or (ii) export any of FIS' Confidential Information to anywhere outside the United States. The provisions of the Purchase Order apply without regard to where the Products or Services are provided or FIS Confidential Information is accessed, stored or processed.

(7) If Provider shall process any Personal Data from FIS or a Client as part of the Services under the Purchase Order regarding individuals domiciled in countries outside of the United States (or to which the GDPR is otherwise applicable), such processing shall be in compliance with FIS' Data Protection Addendum ("**DPA**"), which DPA is incorporated herein by this reference. For the purposes of the DPA (if applicable), FIS and Provider agree that FIS is a Controller, and Provider is a Processor.

(8) In the course of Provider providing Services under the Purchase Order, FIS may from time-to-time provide or make available Data to Provider. The Purchase Order determines the subject matter and the duration of Provider's Processing of Personal Data, as well as the nature and purpose of any collection, use, and other Processing of Personal Data and the rights and obligations of FIS.

(9) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. As a minimum, these should include the requirements required under applicable Data Protection Legislation and the requirements set out in the Purchase Order. Upon request, Provider shall provide a written description of the technical and organizational measures the Provider employs for Processing Personal Data.

(10) Provider must cooperate upon FIS' reasonable request in order to assist FIS with its compliance with applicable privacy Laws, including FIS' handling of Data Subject rights requests.

(11) Where Provider is acting as a Processor under the Purchase Order, at FIS' written request, Provider shall make available to FIS all information reasonably necessary to demonstrate Provider's compliance with the obligations agreed to in the Purchase Order, applicable privacy Laws, and any data protection addenda.

(12) Unless Provider needs identifiable information in order to provide the Products or Services, Provider will deidentify or pseudonymize FIS' Data unless there is a need for the data to be identifiable.

(13) Provider must consider data protection issues as part of the default configuration of its systems, services, products, and business practices. Provider's default configuration will follow privacy by default principles, including data quality, minimization, and accountability. Provider will Process FIS Data in accordance with FIS instructions and only when relevant, minimal, and not excessive.

(14) Provider will provide certification and assurance of its processes and products pursuant to the GDPR.

b. CONSUMER INFORMATION AND PRIVACY. If, in connection with the Purchase Order, Provider receives, stores or accesses any NPI, PHI, Personal Data Payment Card Data, or other information or materials that are subject to the Privacy Regulations and Guidelines, Provider will comply with the applicable requirements of the Privacy Regulations and Guidelines. Provider acknowledges that the Guidelines include provisions regarding the safeguarding of consumer information, response programs and notice in the event of unauthorized access to consumer information, that FIS provides information processing services to Clients subject to the Guidelines, and that FIS may be required to notify Clients, their customers or other third parties of security incidents that result, or are likely to result, in misuse or unauthorized possession or disclosure of NPI, PHI, Personal Data, Payment Card Data or other Confidential Information. Without limiting the foregoing, and in addition to its confidentiality and security obligations as otherwise set forth in the Purchase Order, Provider will (i) ensure the security and confidentiality of such information or materials, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) detect unauthorized access to or use of such records or information, and (iv) protect against unauthorized access to or use of such records or information that would result in harm or inconvenience to any Client or any customer of a Client. Provider represents and warrants that it has and will maintain in place commercially reasonable precautions to safeguard the confidentiality, security and integrity of FIS Confidential Information in a manner designed to meet the requirements of this Section. These precautions will include but will not be limited to (i) contractual restrictions on access to the information by Contractors and Provider's other vendors, (ii) intrusion detection systems on all information systems of FIS maintained or controlled by Provider, and (iii) notification procedures for notifying FIS promptly if a security breach is detected or suspected, as well as other response programs when there is a suspected or detected Breach involving NPI, PHI, Personal Data or Payment Card Data. These precautions will also include, as appropriate, (A) access controls to FIS information systems, including controls to identify and permit access only to authorized individuals and controls to prevent access to FIS Confidential Information through improper means, (B) Provider Personnel controls and training, (C) physical access restrictions at locations where FIS Confidential Information is located, (D) encryption of electronic FIS Confidential Information when appropriate or legally required, and (E) a disaster recovery plan as appropriate to protect against loss or damage to FIS Confidential Information due to potential hazards such as fire or water damage or technological failures. Provider will (1) monitor the foregoing measures with periodic audits or testing and (2) provide copies of the same sufficient to assure FIS or its regulatory authorities that Provider is implementing these precautions, and (3) notify FIS immediately if there is any suspected or actual unauthorized access, use, disclosure or alteration to FIS Confidential Information. Provider will indemnify FIS from, defend FIS against, and pay any final judgments awarded against FIS, resulting from any claim brought by a third party, including but not limited to a customer of FIS, against FIS based on any breach of such privacy Laws, rules or regulations by Provider, including Provider Personnel.

c. CONTROLLED PERSONAL DATA NOTICE. FIS has a Controlled Personal Data Notice which is available for review at http://www.fisglobal.com/Privacy.

PART 4. AFFILIATES, USE, TRANSFER OF PURCHASE ORDER.

a. PURCHASING BY AND TRANSFER TO FIS AFFILIATES. By way of additional Purchase Orders, any FIS Affiliate may purchase, license or otherwise acquire rights in Products or Services to the same extent as FIS has the right to do so, so long as it continues to be an FIS Affiliate, as if such Affiliate were FIS hereunder. Each FIS Affiliate is an intended third party beneficiary hereof and is entitled to rely upon and exercise all rights, representations and warranties made by Provider hereunder to the same extent as if such FIS Affiliate were FIS hereunder. Additionally, FIS or any FIS Affiliate may transfer some or all its rights and obligations under the Purchase Order to any other FIS Affiliate at any time.

b. RIGHTS ACQUIRED. Provider grants to FIS all rights and licenses necessary for the FIS and its Affiliates to use, transfer, pass-through and sell the Product or Services and to otherwise exercise the rights granted under

the Purchase Order with respect to the Product or Service. Notwithstanding any restrictions on transfer of a Product, Service, or their respective associated rights, and notwithstanding acquisition of less than full ownership of any Product or Service by FIS or an FIS Affiliate, the party (FIS or an FIS Affiliate) purchasing, licensing or otherwise acquiring rights in a Product or Service under the Purchase Order may (A) freely transfer the Product or Service to any FIS Affiliate or to FIS (if an FIS Affiliate is the transferor), together with its associated rights, and (B) allow any FIS Affiliate or FIS (if an FIS Affiliate is the transferor) to exercise any rights which the transferor may exercise under the Purchase Order with respect to the Product or Service.

c. CONTINUED EFFECTIVENESS OF ORDERS AND PRODUCT RIGHTS. Expiration of the Term or termination of the Purchase Order for any reason will not terminate any order or agreement that becomes effective under the Purchase Order or the rights acquired by FIS with respect to any Product or Service, including any rights to use the Product or Service and perform other activities in support of such use.

PART 5. PRICING, PAYMENT TERMS, RECORDS.

a. PRICING, PAYMENT TERMS. Unless otherwise specified, the prices for the Products or Services shown on the Purchase Order are the total amounts owed by FIS for the Products or Services. Unless otherwise specified, the prices include, without limitation, all shipping, packing, handling and in-transit insurance charges. Provider will not invoice FIS for any Products or Services or associated expenses prior to (i) completion or acceptance, as applicable, of the requisite delivery or other performance, or (ii) in the case of Services provided on a time and materials basis, the end of the month or other agreed upon time period for which the fees are being charged. FIS may withhold payment of any amount disputed in good faith pending resolution of such dispute. If FIS pays an invoice within fifteen (15) days after receipt of the invoice from Provider, a three percent (3%) discount will apply to the total amount of the invoice; otherwise FIS shall pay an invoice within sixty (60) calendar days following FIS' receipt of a correct and undisputed itemized invoice from Provider. Notwithstanding anything to the contrary in any contract, invoice, document or form issued by Provider, whether signed or otherwise accepted by FIS, FIS will not be obligated to pay interest on late payments, late payment fees or penalties of any kind whatsoever. Provider shall submit all invoices in electronic format through FIS' online invoicing system, as such system may be identified by FIS from time to time.

b. BILLING RECORDS. Provider will create and maintain complete, accurate and up-to-date records and supporting documentation for all invoices and other transactions under the Purchase Order for at least three (3) years following the date of final payment, such records to be maintained in accordance with generally accepted accounting principles and sound business practices. Upon five (5) business days' prior written notice, FIS may verify Provider's compliance with this PART 5. Such verification will be conducted in a manner that minimizes disruption to Provider's business. FIS may use an independent auditor to assist with such verification, provided that FIS has a written confidentiality agreement in place with such independent auditor. Provider will provide to FIS and its auditors accurate electronic and written records, system tool outputs, and other requested system information sufficient to provide verification that Provider's billing invoices are accurate and in compliance with the Purchase Order. FIS will notify Provider in writing if any such verification indicates that Provider is not in compliance with the Purchase Order, and Provider will promptly reimburse FIS for any overpayments made by FIS under the Purchase Order.

c. PRICE INCREASES. During the Term, Provider will not increase the prices applicable to any Products, except as explicitly set forth in the Purchase Order.

d. TAXES. Unless otherwise specified, the prices shown on the Purchase Order do not include all applicable federal, state, and local taxes. All such taxes shall be stated separately on Provider's invoice. If applicable, Provider shall invoice FIS certain indirect taxes imposed by any governmental authority such as sales, use, excise, value added, retailers, occupation and service occupation taxes for the purchase of the products or service which Provider is required by law to collect from FIS, excluding taxes based upon Provider net income, payroll, franchise, or related bases. Provider shall be responsible for all taxes, fees and duties assessed against Provider in connection with the Purchase Order by national or local authorities having jurisdiction over Provider, including at its place of business and at the place of execution and/or performance of the Purchase Order.

PART 6. INDEMNIFICATION.

INDEMNITY. Provider will indemnify, hold harmless and defend at its own expense FIS, its Affiliates and

Contractors, and Clients, and their respective officers, directors and employees, against any action or litigation brought against it by any third party for (i) any claim of infringement of any trademark, patent, copyright or other intellectual property right (including misappropriation of trade secrets) based upon, related to, or arising out of any Products or Services, (ii) any claim of negligence, gross negligence, willful misconduct or failure to comply with applicable Law, rules and regulations by Provider, any Provider Personnel, any Contractor or any Provider Affiliate, in connection with performance under the Purchase Order, or (iii) any claim arising from breach of any obligation under PART 2 (SAFETY AND SECURITY) or PART 3 (SAFEGUARDING OF INFORMATION). Provider's indemnification obligations under this Section will include any and all liabilities, losses, costs, damages, and expenses (including court costs and reasonable attorneys' fees) associated with each Claim. No limitation or exclusion of liability or remedies will be effective with respect to any indemnification or hold harmless obligation of Provider under the Purchase Order.

a. REMEDIAL MEASURES. If an order, judgment or settlement is obtained or reasonably anticipated against FIS' use of any Product or Service on the basis of any Claim, Provider will at its sole cost and expense promptly eliminate the infringement by (i) acquiring a license or licenses on FIS' behalf to provide the necessary rights to FIS, (ii) modifying the Product or Service without impairing its functionality, or (iii) to the extent Provider is unable, exercising its best efforts, to successfully eliminate the infringement by either of the foregoing courses of action, notwithstanding Provider's best efforts, providing FIS with a non-infringing substitute for the Product or Service that provides FIS with the same functionality as the Product or Service.

b. CONDITIONS ON OBLIGATION. The indemnification obligations to an indemnitee with respect to a Claim are contingent upon: (i) the indemnitee, or FIS or Provider (as the case may be) on behalf of the indemnitee, promptly notifying the indemnitor in writing of the Claim; (ii) the indemnitee having sole control over the defense and settlement of the Claim; (iii) the indemnitee reasonably cooperating with the indemnitor during defense and settlement efforts with respect to the Claim; and (iv) the indemnitee not making any admission, concession, consent judgment, default judgment or settlement of the Claim or any part thereof without the prior written consent of the indemnitor, which the indemnitee will not delay or withhold unreasonably.

PART 7. NO PREFERENCES OR EXCLUSIVITY. FIS will not be required in any way to accord preferential or exclusive status to Provider for the Products or Services, and FIS will not be required to purchase or use any Product or Service to the exclusion of other goods or services or to purchase, use or otherwise achieve any minimum volumes or activity with respect to any Product or Service.

PART 8. PERFORMANCE.

a. DELAYS. If Provider's performance is delayed, or is anticipated by Provider to be delayed, by a Force Majeure Event, Provider will promptly notify FIS of (i) the date and details of the Force Majeure Event and the anticipated duration of the Force Majeure Event and the delay, (ii) any material changes in such details or anticipated duration, and (iii) when the Force Majeure Event or delay ends. Provider will use its best efforts to perform in a timely manner, utilizing all resources reasonably required under the circumstances including reasonably available supplies or services from other sources. FIS may terminate the Purchase Order, or the applicable Product or Service, if a Force Majeure Event delays Provider's performance for more than two (2) business days, and no excuse of a performance delay due to a Force Majeure Event will preclude FIS from exercising such termination right.

b. SUBCONTRACTORS. Provider will provide FIS with such information and documentation concerning any Contractor used by Provider to perform Services or provide any part of a Product as FIS requests in writing. Provider will ensure that any such Contractor complies with all obligations of Provider under the Purchase Order. Provider is responsible for all of its obligations under the Purchase Order regardless of where performed or whether performed by any Contractor, and Provider will be liable for the acts and omissions of any Contractor that Provider uses to perform Services or provide any part of any Product.
AUDIT OR INSPECTIONS. Provider will keep complete, accurate, and up-to-date books and records in accordance with generally accepted accounting principles and sound business practices covering all transactions relating to the Agreement. During the Term and for any period FIS is subject to examination with respect to the Products or Services, upon at least ten (10) business days prior written notice from FIS, Provider or its agents will provide FIS, FIS' agents, or any of FIS' regulators, and any Client(s) receiving Products or Services, with access to and any reasonable assistance that they may require with respect to any Provider office or location where the Products are provided or the Services are performed for the

purposes of performing audits or inspections of the Products or Services and the business of FIS relating to the Products or Services. Such audits will be conducted by FIS, FIS' agents, FIS' regulators or Client(s) during regular business hours at any Provider office or location where the Services are performed or Products are provided. If any audit by an auditor designated by FIS, a FIS agent or a regulatory authority results in Provider being notified that Provider or Provider's agents are not in compliance with any Law or any requirement of the Purchase Order, Provider will remedy any such noncompliance within thirty (30) days following such notification. Provider will bear the expense of any such compliance. Any audit hereunder will be subject to the following limitations: (i) use of any third party auditor that is a competitor of Provider will be subject to Provider's prior written approval, such approval not to be unreasonably withheld or delayed; and (ii) FIS or any auditor conducting any such audit will at all times comply with any and all reasonable security and confidentiality guidelines and other policies of Provider with respect to the audit. Provider will have an independent third party annually prepare, and will make available to FIS, a Type II SOC 2 report concerning its operations, systems, controls and procedures, in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 18 and, at FIS' written request, will electronically transmit to FIS a copy of Provider's latest SOC 2 report.

c. COMPLIANCE WITH LAW.

(1) In all circumstances, Provider will comply with, and will ensure that all Products and Services comply with, all Law, including Law relating to export and import, privacy, use, disclosure or transfer of personal information, or security, and Law relating to the employment, health, safety and payment of Provider Personnel. Provider will perform an on-going review of Law applicable to Provider's performance under the Purchase Order and will maintain the features and functions for all standard Products and Services in accordance with all Law applicable to such features and functions, including Law enacted or amended after the effective date of the Purchase Order. Provider will identify and procure all permits, certificates, approvals, licenses, and inspections necessary for Provider's performance under the Purchase Order other than such permits, certificates, approvals, licenses and inspections that FIS is directly responsible for obtaining under the Purchase Order. Without limiting any other obligation of Provider under the Purchase Order, Provider will at all times comply with all Law relating to trade sanctions, export controls, the U.S. Foreign Assets Control Regulations, the U.S. Export Administration Regulations, and the U.S. International Traffic in Arms Regulations.

(2) Non-Discrimination and Affirmative Action. Unless exempt, if Provider is located in the United States, Provider will abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a), and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender-identification or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender-identification, national origin, protected veteran status or disability. If applicable, Provider and its subcontractors will also abide by the requirements of 41 CFR § 61-300.10 regarding veterans' employment reports and the provisions of 29 CFR Part 471, Appendix A to Subpart A regarding posting notice of employee rights.

(3) Sexual Harassment. Provider will promptly notify FIS upon receipt of a complaint regarding the alleged occurrence of any sexual or other harassment incidents, either by or directed at any Provider Personnel, and the parties, where appropriate, will cooperate in investigating said complaint and where necessary take remedial action. Provider represents that Provider has and will continue to maintain anti-harassment policies covering all Provider Personnel, in conformity with applicable federal, state and local Laws. In the event of any claim or legal proceeding relating to a sexual or other harassment incident involving any Provider Personnel, the parties will, where appropriate, cooperate with each other in resolving such claim or legal proceeding.

Anti-Slavery. In performing its obligations under the Purchase Order, Provider shall comply with all applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force including but not limited to the U.K. Modern Slavery Act 2015 and ensure that each of its Contractors shall comply with all applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force including but not limited to the U.K. Modern Slavery Act 2015. If requested by

FIS, Provider shall prepare and deliver to FIS, by no later than fourteen (14) days after such a request, a slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.

(4) Anti-Bribery. Provider shall comply with all applicable laws, statutes, regulations, and codes relating to anti-bribery and anti-corruption including but not limited to the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act 2010. Provider will promptly notify FIS upon becoming aware of a breach of this obligation.

(5) FIS' Code of Conduct. Provider shall comply (and shall procure that all Contractors comply) with FIS' Code of Business Conduct and Ethics located at https://www.fisglobal.com/About-Us/Supplier-Information-Portal.

(6) IR35. If Provider shall assign Provider Personnel that are located in the United Kingdom to perform any part of the Services under the Purchase Order, then the following provision shall apply: The Provider warrants and represents that any staff assigned by the Provider from time to time to provide the Services in the United Kingdom (the "**Assigned Staff**") shall be employed directly by the Provider or by a sub-contractor engaged by the Provider throughout the relevant time and that the Provider or such sub-contractor shall make all payments to such staff as employment income and deduct (and account to HMRC) for any income tax and national insurance contributions through PAYE from such payments. The Provider represents that any such sub-contractor shall not be a personal service company or other intermediary company to which the Income Tax (Earnings and Pensions) Act 2003 Part 2 Chapter 10 applies. The Provider further acknowledges and agrees that notwithstanding any provision in the Contract, if the Provider or any such sub-contractor cease to account for or deduct income tax and national insurance contributions through PAYE from payments made to any Assigned Staff then the Provider will not permit that individual to be involved in the provision of the Services to FIS. The Provider will indemnify FIS and keep FIS indemnified against all losses, fines, penalties, awards, liabilities, costs, damages and expenses (including reasonable legal expenses) (a) arising from FIS being reasonably obliged to pay, or account for, any tax, social security or related penalties, interest or contributions (to the extent permitted by law) in respect of Assigned Staff including (without limitation) as a result of FIS being treated as a "deemed employer" for the purposes of Chapter 7 of Part 2 of Income Tax (Earnings and Pensions) Act 2003 and (b) arising from any employment related claim or any claim based on worker status brought against FIS by any Assigned Staff.

(7) Supplier Diversity. Provider acknowledges and supports FIS' supplier diversity efforts supporting minority business enterprise, woman business enterprise, veteran business enterprise, disabled veteran business enterprise, disabled-owned business enterprises, LGBT owned business enterprises, and Historically Underutilized Business Zone business enterprises (known as HUB Zone business enterprises). Provider shall provide FIS a copy of Provider's supplier diversity program as evidence of Provider's commitment to the participation of such diverse business enterprises in its procurement of goods and services. Provider represents {it is / is not} a diverse supplier. Upon FIS' written request, no more than on a quarterly basis, Provider will provide FIS with Provider's reports summarizing Provider's diversity spend with its suppliers including, but not limited to, total number of diverse suppliers, total spend with diverse suppliers and percentage of total spend attributed to diverse supplier types. Provider shall provide such reports within thirty (30) calendar days of FIS' written request for such information.

d. USE OF FIS OR CLIENT NAMES. Provider will not use FIS' names, logos, trademarks or stock exchange ticker symbol, or in connection with the Purchase Order, those of any Client, unless pre-approved in writing by FIS. Provider will not make any press release or other similar communication that mentions or implies a relationship between Provider and FIS, or between Provider and a Client in connection with the Purchase Order, unless pre-approved in writing by FIS.

e. WARRANTIES. Provider represents and warrants to FIS: (a) that it has full right and authority to perform its obligations and grant the rights and licenses granted under the Purchase Order; (b) that it has not assigned, transferred, or entered into any other relationship by which it purports to assign or transfer, any right, title or interest to any technology, process, material or intellectual property right that would be in conflict with the terms of the Purchase Order, and that Provider will not do so in the future; (c) (c) that neither the execution and delivery of the Purchase Order nor the other documents and instruments to be executed and delivered by Provider under the Purchase Order nor the consummation of the transactions contemplated by the Purchase Order will (i) violate any Law, including injunction or decree of any court, (ii) require any action by Provider to

obtain or give any authorization, consent, approval, exemption or other action by or notice to any court, administrative or governmental agency, instrumentality, commission, authority, board or body (or if so required, Provider has taken all such actions and obtained all needed and necessary authorizations, consents, approvals, and exemptions), or (iii) violate or conflict with, or constitute a default (or an event which, with notice or lapse of time, or both, would constitute a default) under, any term or provision of Provider's charter or bylaws or any contract, license, or legal restriction of any kind or character to which Provider is a party or by which Provider or any of its assets or properties may be bound or affected; (d) that there is no action, suit, arbitration proceeding, investigation or inquiry pending or threatened against Provider, its business or any of its assets, and that Provider does not know or have grounds to know, of any basis for any such actions, suits, arbitrations, proceedings, investigations or inquiries, that would affect its ability to perform its obligations under the Purchase Order; (e) that during the Term, Provider will maintain an adequate and trained staff of employees and adequate and proper facilities, resources and systems in order to provide the Software, perform the Services and otherwise deliver the Products to FIS as mutually agreed upon pursuant the Purchase Order; and (f) that it will not introduce or allow any Destructive Elements into the Services or Products, or into the systems of FIS or any of FIS Clients or their customers. Without limitation of the foregoing, Provider warrants and covenants that it will use best efforts to avoid the coding or introduction of Destructive Elements into any systems used to provide Services or Products. Provider will assist FIS with mitigation of any loss of operational efficiency or loss of data caused by such Destructive Elements. Upon learning of or discovering a cyber or information-security threat or vulnerability to FIS systems or to FIS Clients or their customers (including without limitation notifications received from security researchers, industry resources, or bug bounty programs), Provider will promptly notify and cooperate with FIS and take all reasonable and necessary steps to isolate, mitigate, and remediate such known or suspected threat or vulnerability and reimburse FIS for its actually incurred costs in connection with such bug bounty programs.

f. INSURANCE.

(1) Insurance. The insurance requirements set forth below provide the minimum coverage amounts for certain types of insurance, together with certain and other requirements relating to such insurance and will be part of the Purchase Order. Provider agrees that prior to executing the Purchase Order, and within ten (10) days of each subsequent policy renewal, Provider will provide FIS with Provider's certificate(s) of insurance evidencing that the coverage and policy endorsements described in this Section are maintained in force with Provider's insurer(s) having A.M. Best ratings of at least A-(VIII). Provider will maintain such insurance and comply with such other obligations, at its own expense, at all times the Purchase Order is in effect and for at least one (1) year following the completion of the engagement. FIS may require additional insurance coverage and requirements in connection with a particular engagement, as set forth in the applicable Purchase Order.

(2) Types and Minimum Amounts of Insurance Coverage.

(a) Commercial general liability insurance including premises & operations, products/completed operations, contractual, broad form property damage, and personal injury with a combined single limit of at least One Million and 00/100 U.S. Dollars ($1,000,000) per occurrence and Two Million and 00/100 U.S. Dollars ($2,000,000) general aggregate.

(b) Business automobile liability insurance for all owned, non-owned, borrowed, leased, and hired vehicles to be used under the Agreement, with a combined single limit of at least One Million and 00/100 U.S. Dollars ($1,000,000) each accident.

(c) Workers' compensation with alternate employer endorsement and including at least One Million and 00/100 U.S. Dollars ($1,000,000) employers liability insurance coverage,

(d) Umbrella (excess) liability insurance coverage in an amount of at least Five Million and 00/100 U.S. Dollars ($5,000,000) per occurrence.

(e) Property insurance against all risks of physical loss or damage to any property of FIS in the care, custody, or control of Provider.

(f) Professional liability insurance in an amount of at least Ten Million and 00/100 U.S. Dollars ($10,000,000) including coverage for network security liability and privacy liability.

(g) Commercial crime insurance including employee dishonesty coverage in an amount of at least Five Million and 00/100 U.S. Dollars ($5,000,000).

(3) Other Insurance Obligations. Provider or its insurers will provide thirty (30) days written notice to FIS prior to cancellation or material change of any such policy. Except with respect to the gross negligence of FIS, Provider's policies will be primary and non-contributing with respect to any other insurance or self-insurance which may be maintained by FIS. FIS will be named as an additional insured under the commercial general liability, automobile liability, umbrella and professional liability policies, as well as a loss payee under the commercial crime policy described above. Provider and its insurance carriers will waive subrogation with respect to the workers' compensation, employers liability, commercial general liability and automobile liability policies. Provider will be responsible to ensure that any Provider Contractors maintain in force coverage as outlined in this Section or that coverage is extended to such Contractors under Provider's policies. The carrying of the above-described coverage will in no way be interpreted as relieving Provider of any other responsibility or liability under the Purchase Order or any applicable Law.

g. THIRD PARTY SOFTWARE. In connection with the provision of Products or Services to FIS, Provider has not and shall not use, incorporate, or integrate any third party computer software except as set forth on the Purchase Order or with FIS' prior written consent. Any software or component thereof made available pursuant to an open source license must be identified by name, version, and license type in the Documentation. Nothing contained in an open source license is intended or shall be construed to alter Provider's license grant or infringement indemnification, warranty, or other obligations under these Purchase Order Terms for such software or component, nor limit FIS' rights and remedies in connection therewith. Nothing contained under these Purchase Order Terms is intended or shall be construed to limit FIS' independent license or other rights under an applicable open source license. Provider represents and warrants that, to the extent that any open source code is embedded or integrated into the software, no such use of open source shall cause FIS' material, Confidential Information, data, information, processes, or systems (or any intellectual property rights in any of the foregoing) to be subjected to open source software license terms, including any 'copyleft' terms that: (a) grant, or purport to grant, to any third party any right to or in FIS' or any of its Affiliates' respective intellectual property rights; or b) require FIS or any of its Affiliates to make any source code (or any part or derivative work thereof) available to third parties under any circumstances

PART 9. LIMITATION OF LIABILITY.

a. Limitation on Direct Damages. Except for FIS' obligation to pay fees to Provider, FIS' TOTAL LIABILITY AND PROVIDER'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF ANY TYPE WHATSOEVER, ARISING OUT OF THE PURCHASE ORDER, WILL BE LIMITED IN ALL CASES AND IN THE AGGREGATE TO PROVEN DIRECT DAMAGES IN AN AMOUNT NOT TO EXCEED THE PRICE PAID BY FIS TO PROVIDER FOR THE SPECIFIC SERVICE OR PRODUCT PROVIDED BY PROVIDER HEREUNDER FOR THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE THE CLAIM AROSE, WHICH UNDER NO CIRCUMSTANCES WILL EXCEED, IN THE AGGREGATE, THE AMOUNT PAID BY FIS TO PROVIDER UNDER THE PURCHASE ORDER. UNDER NO CIRCUMSTANCES WILL FIS HAVE ANY OBLIGATION TO PROVIDER UNDER ANY THEORY OF LIABILITY OR OTHERWISE FOR ANY LOSSES CAUSED DIRECTLY OR INDIRECTLY, IN WHOLE OR IN PART, BY (I) PROVIDER, (II) A THIRD PARTY OTHER THAN FIS' AUTHORIZED AGENTS, (III) ADHERENCE TO PROVIDER'S INSTRUCTIONS OR REQUIREMENTS, (IV) IMPROPER OR INCOMPLETE SYSTEMS, DATA, SOFTWARE OR EQUIPMENT SUPPLIED BY PROVIDER, (V) A FORCE MAJEURE EVENT OR (VI) ANYTHING NOT ATTRIBUTABLE TO FIS OR UNDER FIS' ABILITY TO CONTROL.

b. No Indirect Damages. NEITHER FIS NOR ANY FIS AFFILIATE WILL HAVE LIABILITY TO PROVIDER FOR ANY SPECIAL, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, REVENUES, DATA OR USE), EVEN IF ADVISED OF THE POSSIBILITY THEREOF. PROVIDER WILL NOT BRING ANY CLAIM HEREUNDER MORE THAN EIGHTEEN (18) MONTHS AFTER THE DATE THE CAUSE OF ACTION ACCRUES.

c. Liability Limited. Liability for damages will be limited and excluded even if any exclusive remedy provided for under the Agreement fails of its essential purpose.

d. Provider Liability. PROVIDER'S LIABILITY WILL BE UNLIMITED WITH RESPECT TO DEATH, PERSONAL INJURY, PROPERTY DAMAGE, OR ANY INDEMNIFICATION OBLIGATION ARISING UNDER THE PURCHASE ORDER. NO LIMITATION OF LIABILITY WILL APPLY TO LIMIT PROVIDER'S LIABILITY TO LESS THAN THE TOTAL AMOUNT PAID OR PAYABLE UNDER THE PURCHASE ORDER OR ONE MILLION DOLLARS ($1,000,000), WHICHEVER IS GREATER.

PART 10. OWNERSHIP.

a. FIS Ownership. Any and all deliverables, inventions and works pursuant to or resulting from the Services will be considered works made for hire by Provider and will, upon creation, be owned exclusively by FIS. To the extent that such deliverables, inventions or works may not be considered works made for hire, Provider hereby assigns, without the necessity of further consideration, all of its right, title and interest to FIS and FIS will be entitled to hold same in its own name on all applicable patents, registrations or copyrights.

b. Assignment. If and to the extent that Provider may, under applicable Law, be entitled to claim any ownership interest, or moral rights, in the deliverables, inventions or works related to the Services, Provider hereby transfers, grants, conveys, and relinquishes (and shall cause its Provider Personnel to transfer, grant, convey, and relinquish with retroactive effect to the start date of the Services) exclusively to FIS all of its right, title and interest under patent, copyright, trade secret, and trademark Law, to the extent allowable by Law, in perpetuity or for the longest period otherwise permitted by Law.

c. Other Necessary Documents. Provider will sign upon request (and shall cause its Provider Personnel to transfer, grant, convey, and relinquish with retroactive effect to the start date of the Services), all documents necessary to vest title in FIS to any intellectual property rights associated with the Services, deliverables, inventions or works related to the Services. Provider will also sign upon request, any document necessary for the filing and prosecution of patent, trademark or copyright applications in the United States and elsewhere, including divisional, continuation, revival, renewal or reissue application. Provider will cooperate and assist FIS in preparing, filing and prosecuting any and all such patent, trademark and copyright applications during the Term and for two (2) years following its termination. FIS will bear all costs associated with the prosecution of such patent, trademark or copyright applications.

d. Pre-existing Works. To the extent that any preexisting rights are embodied or reflected in the Services, deliverables, inventions or works related to the Services, Provider hereby grants to FIS an irrevocable, perpetual, non-exclusive, world-wide, royalty-free right and license to: (i) use, execute, reproduce, display, perform, distribute copies of and prepare derivative works based upon such preexisting rights; and (ii) authorize others on FIS' behalf to do any or all of the foregoing.

PART 11. ESCALATION PROCEDURE; DISPUTE RESOLUTION; ADDITIONAL REMEDIES.

a. Escalation Procedure. FIS and Provider will first attempt to resolve any dispute, difference, controversy or claim under this Agreement between their respective project managers identified in the Agreement. Each party shall escalate any and all unresolved disputes by notifying the other party in writing that it desires to elevate the matter to the FIS-designated executive officer of FIS and the Provider-designated executive officer of Provider for resolution. Upon receipt by the other party of such written notice, the matter shall be so elevated and the FIS-designated executive officer of FIS and the Provider-designated executive officer of Provider shall negotiate in good faith and each use its reasonable best efforts to resolve any remaining issues. The location, format, frequency, duration and conclusion of these elevated discussions shall be left to the discretion of the representatives involved. Upon mutual agreement, the representatives may utilize other alternative dispute resolution procedures to assist in the negotiations. All discussions and correspondence among the representatives for purposes of these negotiations shall be treated as Confidential Information developed for purposes of settlement, exempt from discovery and production, which shall not be admissible in any subsequent proceedings between the parties. Documents identified in or provided with such communications, which are not prepared for purposes of the negotiations, are not so exempted and may, if otherwise admissible, be admitted in evidence in such subsequent proceeding. If the disputed matter remains unresolved after the escalation procedure set forth above, then either party may, within thirty (30) calendar days after the

representatives have met to address such matter, request binding arbitration of the issue in accordance with subsection (b) below.

b. Alternative Dispute Resolution. If FIS is, as of the Purchase Order Effective Date, headquartered in the European Economic Area, United Kingdom or Switzerland then only subsection (b)(2) below applies. If FIS is, as of the Purchase Order Effective Date, headquartered outside of the Americas or the European Economic Area, United Kingdom or Switzerland then only subsection (b)(3) below applies. In all other cases, subsection (b)(1) below applies.

(1) FIS and Provider will settle any dispute, difference, controversy or claim arising out of or relating to the Purchase Order by binding arbitration before a single arbitrator in Jacksonville, Florida in accordance with the Commercial Arbitration Rules (including Procedures for Large, Complex Commercial Disputes) of the American Arbitration Association. Judgment on any resulting award may be entered into by any court having jurisdiction over the parties or their respective property. The arbitrator will decide any issues submitted in accordance with the provisions and commercial purposes of the Purchase Order, and will not have the power to award damages in excess of the limitations set forth in, or damages excluded by, the Purchase Order. FIS and Provider may elect to engage in non-binding mediation as a first alternative to binding arbitration or litigation as provided in this subsection (b)(1). Any such election must be mutual and reflected in a writing signed by both parties. Each party will bear its own costs in arbitration, and in any such mediation, and the parties will share equally all third party arbitration or mediation costs, unless otherwise mutually agreed upon in writing by the parties. Subject to the above arbitration requirement, venue for any litigation arising out of or otherwise relating to the Purchase Order will be in state and federal courts of competent jurisdiction located in Duval County, Florida, which will have exclusive jurisdiction over such litigation. Nothing in the Purchase Order will prevent either party from seeking any stay of proceedings or preliminary or temporary injunctive relief from a court of competent jurisdiction either to enforce the parties' agreement to arbitrate or mediate any dispute under this subsection (b)(1) or to enjoin the other party's breach of its information security or confidentiality obligations under the Purchase Order. THE PARTIES HEREBY IRREVOCABLY WAIVE ANY AND ALL RIGHTS TO TRIAL BY JURY IN ANY LEGAL PROCEEDING ARISING OUT OF OR RELATING TO THE AGREEMENT.

(2) The Purchase Order and any dispute, difference, controversy, or claim arising, directly or indirectly, out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) is governed by, and shall be construed and enforced in accordance with, the laws of England and Wales excluding choice of law. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute, controversy or claim arising, directly or indirectly, out of or in connection with the Purchase Order, or the breach, termination or validity thereof (including non-contractual disputes or claims). The Contracts (Rights of Third Parties) Act 1999 shall not apply to the Purchase Order.

(3) The Purchase Order and any dispute, difference, controversy, or claim arising, directly or indirectly, out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) is governed by, and shall be construed and enforced in accordance with, the laws of England and Wales excluding choice of law. Each party irrevocably agrees that the any dispute, controversy or claim arising, directly or indirectly, out of or in connection with the Purchase Order, or the breach, termination or validity thereof (including non-contractual disputes or claims), shall be referred to and finally resolved by the International Court of Arbitration of the International Chamber of Commerce under the Rules of Arbitration of the International Chamber of Commerce ("**ICC**") for the time being in force, which rules are deemed to be incorporated by reference in this Section. The location and seat of the arbitration shall be: (i) London if Client is headquartered in Middle East or Africa; and (ii) Singapore if Client is headquartered in Asia Pacific. There shall be one arbitrator. The arbitrator shall be agreed between the parties. Failing agreement, or if the arbitrator selected is unable or is unwilling to act, the appointing authority shall be the ICC. The arbitration proceedings shall be conducted in English. The decision of the arbitrator shall be final and binding upon both parties and shall be enforceable in any court of law. Each of the parties waives irrevocably their right to any form of appeal, review or recourse to any state court or other judicial authority, insofar as such waiver may be validly made. Notwithstanding anything to the contrary in the Purchase Order, either party may at any time seek an interim injunction or other interlocutory relief in a court of competent jurisdiction in order to protect any urgent interest of such party, including, but not limited to, the

confidentiality provisions of this Purchase Order. The law governing the arbitration agreement contained in this Section, the arbitration, and the conduct and procedure of the arbitration, shall be the laws of England and Wales. The Contracts (Rights of Third Parties) Act 1999 shall not apply to the Purchase Order.

c. Additional Remedies. Any and all rights and remedies which either party may have under the Purchase Order, at Law or in equity, will be cumulative and will not be deemed inconsistent with each other, and any two (2) or more of all such rights and remedies may be exercised at the same time insofar as permitted by Law. Due to the likelihood of irreparable injury, FIS will be entitled to an injunction prohibiting any breach of the Purchase Order by Provider.

PART 12. AMENDMENTS; AUTHORIZED REPRESENTATIVES. The Purchase Order may only be modified only by a written instrument signed by duly authorized representatives of both parties.

PART 13. USAGE AND INTERPRETATION.

a. ENGLISH LANGUAGE. English will be the language of the Purchase Order. Translation of the Purchase Order, its attachments, schedules, exhibits, correspondence, documents, invoices, notices or other communications related to the Purchase Order, or the transactions thereunder, into another language will be at the sole risk of the translating party. If any conflicts arise between the English version of the Purchase Order and a translated version, the English version will prevail. If permitted under local Law, all communications pursuant to the Purchase Order will be conducted in the English language. Unless the context clearly indicates otherwise, (i) references to a party's agreement, consent, notice, request or approval mean written and signed agreement, consent, notice or approval, (ii) the words "will" and "shall" have the same meaning, which is obligatory, and (iii) the word "including" means "including, without limitation" so that it does not limit the scope of the word or phrase to which it is applied.

b. WEB-BASED PROVISIONS, PASSIVE CONTRACTS, INVOICE TERMS. The effectiveness of the Purchase Order, or of any statement or other contract made under the Purchase Order, will not be conditioned upon FIS becoming bound by (i) a reference in the Purchase Order to one or more documents maintained by Provider and made available to FIS at a Web page, by email distribution or in any other manner; (ii) a "click-through", "shrink wrap" or similar mechanism presented by Provider (whether in the past, present or future) involving the use of an action other than actual signature or electronic signature (as recognized by Law) to cause agreement to terms and conditions presented by Provider; or (iii) as part of an invoice or similar administrative document. The parties understand and agree that any such documents, terms and conditions will be only for (A) informational purposes or to set forth obligations of or rights granted by the Provider or its Affiliates, (B) that neither FIS nor any FIS Affiliate will be bound by any contractual obligation that might otherwise arise from any such reference or mechanism, whether under or in connection with the Purchase Order or otherwise, and (C) that any such documents, terms and conditions will in any event be subject to the Purchase Order, including these terms.

c. WAIVER. Failure by FIS to enforce the performance of any of the provisions of the Purchase Order shall neither be deemed to be a waiver of its rights hereunder nor shall it affect the validity of the Purchase Order in any way. Any waiver by FIS to any breach of the Purchase Order shall be specific to such particular breach and shall not bind the parties in respect of any subsequent breach by Provider, even if such subsequent breach is identical or similar.

PART 14. RELATIONSHIP OF THE PARTIES. Provider is an independent contractor without authority to bind FIS by contract or otherwise, and neither Provider nor Provider's employees or agents are agents or employees of FIS, and Provider hereby indemnifies and holds FIS harmless against any claim by such employees or agents alleging an employment relationship with FIS.

PART 15. ENTIRE UNDERSTANDING; MISCELLANEOUS. The Purchase Order (including, for the avoidance of doubt, these Purchase Order Terms) and any other schedules, exhibits and addenda hereto states the entire understanding between the parties with respect to its subject matter, and supersedes all prior proposals, marketing materials, negotiations, representations (whether negligently or innocently made), agreements and other written or oral communications between the parties with respect to the subject matter of the Purchase Order. Nothing in these Purchase Order Terms shall limit or exclude any liability for fraud or fraudulent misrepresentation. The parties hereto

agree to perform all acts and execute all supplementary instruments or documents which may be necessary or desirable to carry out the provisions of the Purchase Order and these Purchase Order Terms. The Purchase Order and these Purchase Order Terms will not be construed more strongly against either party regardless of who is more responsible for its preparation. If there is a conflict between a part of the Purchase Order or these Purchase Order Terms and any present or future Law, the Purchase Order and these Purchase Order Terms will be curtailed only to the extent necessary to bring it within the requirements of that Law

PART 16. SURVIVAL. The rights and obligations set forth in PART 2.c (INFORMATION SECURITY AND INTERNAL CONTROLS), PART 3 (SAFEGUARDING OF INFORMATION), PART 5 (PRICING, PAYMENT TERMS, RECORDS), PART 6 (INDEMNIFICATION), PART 8.e (COMPLIANCE WITH LAW), PART 9 (LIMITATION OF LIABILITY) and PART 11 (ESCALATION PROCEDURE; DISPUTE RESOLUTION; ADDITIONAL REMEDIES) of these Purchase Order Terms, and those provisions of these Purchase Order Terms which by their express terms extend beyond expiration of the Term or termination of the Purchase Order, or which by their nature so extend, will survive and continue in full force and effect after the expiration of the Term or the termination of the Purchase Order.

APPENDIX A - THIRD-PARTY SERVICE PROVIDER INFORMATION SECURITY REQUIREMENTS

THIRD-PARTY SERVICE PROVIDER INFORMATION SECURITY REQUIREMENTS

Version Date: July 6, 2022

1. INTRODUCTION

These Third-Party Service Provider Information Security Requirements ("**Requirements**") describe Third-Party Service Provider's obligations with respect to information security and data protection in relation to the Services, Software, and/or Deliverables provided by Third-Party Service Provider to FIS under the agreement between FIS or FIS' affiliate(s) and Third-Party Service Provider which incorporates these Requirements by reference ("**Agreement**"). The term "**Third-Party Service Provider**" shall mean a third-party providing Software or Services to FIS or a FIS Client and who is identified by either their entity name or the defined terms "Vendor", "Supplier", "Provider", or "Consultant" in the Agreement. Terms capitalized and used in these Requirements will have the meanings ascribed to them under the Agreement unless specifically provided for in these Requirements otherwise. In the event an entity other than Third-Party Service Provider does so under a contract with Third-Party Service Provider or otherwise for or on behalf of Third-Party Service Provider, Third-Party Service Provider will ensure by contract or otherwise that the following provisions apply correspondingly to the other entity for the benefit of FIS. To the extent of any conflict or inconsistency between the provisions of these Requirements and any provision of the Agreement, the provisions of these Requirements prevail and take precedence over such conflicting or inconsistent provisions in the Agreement.

2. ORGANIZATIONAL PRACTICES

Third-Party Service Provider shall implement and maintain commercially reasonable administrative, technical, organizational, and physical safeguards and measures ("**Information Security Policies**"), described throughout these Requirements, that are designed (1) to prevent the compromise or unauthorized disclosure of FIS Confidential Information, Client Confidential Information, and Personal Data (collectively, "**Protected Data**"), including its loss, corruption, destruction, or mis-transmission; (2) to protect against any anticipated threats or hazards to the security or integrity of Protected Data it stores, processes, or otherwise controls; and (iii) to protect against unauthorized access to or use of Protected Data.

Third-Party Service Provider is responsible for developing, implementing, and maintaining Information Security Policies in accordance with Good Industry Practice that are designed to ensure compliance with (1) all Laws relating to the privacy, confidentiality and security of Protected Data to the extent applicable to the Software, Services, and/or Deliverables provided by Third-Party Service Provider under the Agreement; (2) the obligations set forth in these Requirements; and (3) all applicable provisions of the Agreement. Third-Party Service Provider's information security practices shall also be compliant with International Organization for Standardization ISO 27001:2013, and its successor standards.

Third-Party Service Provider shall update its Information Security Policies from time to time in response to evolving information security threats in accordance with leading information security industry standards (e.g., National Institute of Standards and Technology ("**NIST**")). Such updates must be at least an equivalent or increased level of security compared to what is described in these Requirements, and Third-Party Service Provider will periodically provide FIS with a summary of any updates upon FIS' written request.

Third-Party Service Provider will review, assess, evaluate, and test the security and effectiveness of its Information Security Policies regularly and not less than annually. Third-Party Service Provider will notify FIS of any and all Information Breaches to Third-Party Service Provider's information security promptly and no later than twenty-four (24) hours following discovery of such Information Breach and work with FIS management, as reasonably requested, to identify the root cause of the incident and the potential impact to FIS, its Clients, their customers, and data subjects. Third-Party Service Provider will also mitigate any adverse effects.

3. GENERAL SECURITY CONTROLS

3.1 THIRD PARTY SERVICE PROVIDER FACILITIES – ACCESS CONTROLS, FACILITY RESTRICTIONS; EMERGENCY PROCEDURES. Physical security measures implemented at Third-Party Service Provider's data center facilities, buildings, office spaces, and secured areas within the facility from which Third-Party Service Provider provides the Services ("**Facilities**") must be designed to protect employees, visitors, and assets used in the provision of Software, Services, and/or Deliverables under the Agreement. Access to Facilities must be monitored and restricted, using Physical Security Controls. "**Physical Security Controls**" consist of a combination of access control systems, monitoring systems, security officers and procedures for controlling access to buildings and sensitive or restricted areas.

Access control systems shall be utilized to provide Facility physical security and protection, including individual badge identification, doors protected by an electronic badge reader or locked with limited access to the physical key, closed circuit camera monitoring, and onsite physical security guards stationed in strategic locations. Onsite physical security guards shall be stationed in strategic locations at Facilities 24 hours a day, seven days a week. Badges and keys shall only be distributed in accordance with documented organizational procedures aligned with leading information security industry

standards (e.g., ISO 27001). Visitors shall be screened prior to admittance, provided a visitor badge, and require an escort in sensitive areas in accordance with Information Security Policies.

Every access control system shall provide for real-time monitoring of all electronic badge accesses across the monitored Facilities, onsite security officer acknowledgement of system identified error codes or issues, and shall be tied to centralized servers communicating the exact date and time stamp for each entry (utilizing network time protocol). Automated database backups shall be performed daily and replicated on the secondary server. Alarm systems shall be in place to notify appropriate individuals of potential threats.

Third-Party Service Provider shall regularly test its emergency procedure protocols. For data centers, Third-Party Service Provider must ensure to maintain automatic early-warning sensors (e.g., fire, water, temperature and humidity), independent air conditioning systems and fire suppression systems. Mission-critical hardware shall be protected by an emergency power supply system with batteries and backup generators. Hazardous or combustible materials shall be kept at a safe distance from information assets. Secure shred bins are provided for the proper disposal of hard copy documentation and other small media thorough-out the campus.

3.2 PERSONNEL. Third-Party Service Provider shall ensure that processes employed in the provision of the Services are staffed in such manner as to prevent conflicts of interest, fraud or error by invoking appropriate separation of duties. Third-Party Service Provider must assign all personnel to mandatory security awareness and data protection training on an annual basis. Third-Party Service Provider shall ensure that persons authorized to process the Protected Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. All personnel with access to sensitive information shall be required to follow a clean desk and clear screen standards such that Protected Data is controlled and/or protected at all times. Third-Party Service Provider must also have formal personnel disciplinary procedures in place to address policy violations. A terminated personnel's access to Third-Party Service Provider's facilities and Third-Party Service Provider's systems containing Protected Data must be promptly suspended upon termination.

3.3 ELECTRONIC MAIL. Third-Party Service Provider shall scan incoming emails and attachments prior to allowing them into any Third-Party Service Provider's environment. Third-Party Service Provider shall also use industry-leading software to control what files are allowed or blocked as attachments to protect against malicious executable files being delivered and/or opened.

3.4 AUTHENTICATION AND REMOTE ACCESS. The level of authentication required to access a particular Third-Party Service Provider environment shall be based on the type of data protected within that environment. Third-Party Service Provider must only permit authorized persons to access any Third-Party Service Provider systems in accordance with the Information Security Policies. User authentications (i.e., username and password) shall be bound to the respective user and may not be shared. The use of an emergency user account must be documented and logged. Remote access to FIS' systems shall require the use of multi-factor authentication.

3.5 PASSWORDS. Third-Party Service Provider must utilize complex passwords. User accounts must be locked after a defined number of abortive or unsuccessful logon attempts. If a password is possibly disclosed, it must be changed without undue delay. In accordance with the Information Security Policies, Third-Party Service Provider will employ processes to minimize the risk of unauthorized or no longer needed user accounts in the systems by performing audits or reviews of user accounts and immediately revoke authentication rights, upon determining that user is not required.

3.6 DATA CLASSIFICATION, RETENTION, AND CONTROLS. Third-Party Service Provider's Information Security Policies address the confidentiality, integrity, security, availability, retention and disposal of Protected Data. Third-Party Service Provider will take reasonable steps to determine access to Protected Data. Third-Party Service Provider's policy governing access management must be based on the "principle of least privilege," which calls for authorized users to access only the minimum level of Protected Data required to satisfy the user's job responsibilities. All Third-Party Service Provider employees and vendors with access to Protected Data are required to comply with secure deletion standards in alignment with leading information security industry standards (e.g., NIST *Guidelines for Media Sanitization)*. Third-Party Service Provider will store Protected Data only for as long as necessary to achieve the purposes for which it was collected, for the duration of the contractually committed time period as set forth in the Agreement, or as required by applicable Laws. Third-Party Service Provider will also have processes to promptly return and/or erase all data in Third-Party Service Provider's possession or control, at the request and option of FIS, in a manner that maintains its confidentiality and integrity, as agreed between the parties.

3.7 MONITORING SYSTEMS AND PROCEDURES / LOGGING. Third-Party Service Provider must use a real-time event management system ("**SIEM**") to monitor its networks and servers via system logs, intrusion detection/prevention systems, data loss prevention, file integrity monitoring and firewall logs on a 24-hour per day basis. Third-Party Service Provider will perform reasonable logging, monitoring, or record keeping of user activity where legally permissible and in accordance with Third-Party Service Provider's applicable information retention standards.

3.8 VENDOR MANAGEMENT. Third-Party Service Provider will conduct a risk assessment for its third-party contractors, subcontractors, and its suppliers engaged in the provision of Services under the Agreement ("**Suppliers**") to validate compliance with these Requirements. Third-Party Service Provider's risk assessment shall require its Suppliers to confirm if they have appropriate contracts in place with their vendors that store, process, transmit, manage or access

Protected Data. Third-Party Service Provider may allow such Suppliers to access, store, transmit, manage, or process Protected Data, only to the extent permissible under the Agreement and applicable Laws. Third-Party Service Provider will require Suppliers to agree to data protection agreements to obligate such Suppliers to comply with applicable data protection Laws, which data protection agreements shall contain terms that offer at least the same protection for Protected Data as the data protection agreement between FIS and Third-Party Service Provider. Suppliers shall as a minimum implement appropriate technical and organizational measures to verify a level of security appropriate to the risk.

3.9 APPLICATIONS AND SYSTEMS DEVELOPMENT. Third-Party Service Provider uses system development lifecycle and system change procedures, which include requirements for code review and secure coding practices. Development and testing environments must be segregated and firewalled from Third-Party Service Provider's production environment. Version control software is utilized for the management and deployment of code through appropriate support groups. Third-Party Service Provider shall apply measures for verifying system configuration, including default configuration. Third-Party Service Provider must consider data protection issues as part of the design and implementation of systems, services, products and business practices (i.e., privacy by design and by default).

3.9.1 DYNAMIC APPLICATION SCANNING. Third-Party Service Provider will conduct dynamic application scanning on internet facing browser applications, which includes scanning for vulnerabilities listed in the SANS Top 20 or OWASP Top 10 or its successor current at the time of the dynamic application scan. Third-Party Service Provider will provide a summary of the dynamic application scan to FIS upon request. The scan will be performed using an industry standard tool and occur no less than twice a year. Third-Party Service Provider will (at its own cost) remediate any findings in accordance with FIS remediation timeframe policy.

3.9.2 STATIC APPLICATION SECURITY TESTING. Third-Party Service Provider must conduct static application security scanning, which include scanning for vulnerabilities listed in the SANS Top 20 or OWASP Top 10 or its successor current at the time of the static application security scan. Third-Party Service Provider will provide a summary of the static application security scan to FIS upon request. The scan is performed using an industry standard tool. Third-Party Service Provider will (at its own cost) remediate any findings in accordance with FIS remediation timeframe policy.

4. SERVICE-SPECIFIC SECURITY CONTROLS

4.1 CONTROL APPLICABILITY. The following logical control and security requirement is only applicable if Third-Party Service Provider is (a) storing or processing Protected Data on its network, or (b) remotely accessing FIS' or a FIS Client's Protected Data, or FIS' or a FIS Client's network with FIS or Client network access credentials in connection with the Services under the Agreement.

4.1.1 NETWORK SECURITY. Third-Party Service Provider will employ a defensive model when building networks (including firewalls) in a multi-tiered approach and use separate layers of presentation, business logic and data when considered necessary in accordance with the Information Security Policies. Connection between networks shall be limited to those ports and services required for Third-Party Service Provider to support, secure, monitor and perform the Services under the Agreement. Such defensive model will include robust processes to ensure that changes to the premises, networks, systems and software used to supply the Services are appropriately evaluated, tested and implemented to limit the potential of service degradation. Network firewall rules are to be reviewed at least every six (6) months. Third-Party Service Provider must maintain separate environments between test and production systems and ensure that no FIS production data is used in test systems.

Third-Party Service Provider will use network intrusion detection and/or prevention systems to monitor and or prevent threats to the FIS environment. Third-Party Service Provider will monitor these threats constantly during the Term of the Agreement and until all Protected Data is returned or deleted, as the case may be pursuant to the Agreement or Engagement Document, or all access credentials are cancelled, whichever is later.

Where all, or part of, the Services are provided using online services (i.e., accessible via the internet), the Third-Party Service Provider must deploy web application firewall ("**WAF**") and ensure that adequate protection is in place to mitigate the risk of denial-of-service threats.

Third-Party Service Provider shall not purposely create back doors or similar programming that could be used to access the Protected Data. Third-Party Service Provider shall not purposefully create or change its business processes in a manner that facilitates access to Protected Data by any foreign government.

4.2 CONTROL APPLICABILITY. The following logical control and security requirements are only applicable if Third-Party Service Provider is (a) storing or processing Protected Data on its network, or (b) remotely accessing FIS' or a FIS Client's Protected Data, or FIS' or a FIS Client's network with FIS or Client network access credentials and without FIS or FIS Client issued equipment in connection with the Services under the Agreement.

4.2.1 HOST AND SERVER SECURITY. Third-Party Service Provider will harden its operating systems (e.g., all default passwords are changed and unneeded functionality is disabled or removed) in accordance with leading information security industry standards (e.g., NIST, the Center of Internet Security). Third-Party Service Provider must adhere to the concept of "least-privileged" access, file permissions do not include world writeable ability, administrative or "root" access

is limited to the console only, and only those network ports that are necessary to provide the services are opened. For database installations, Third-Party Service Provider must use security at a table and row level, based upon the placement of a system and its role in the environment. Third-Party Service Provider must have anti-malware software enabled on its operating systems when they are available and supported by commercially available anti-malware solutions such as endpoint detection and response ("**EDR**") or extended detection and response ("**XDR**") solutions.

Access to Third-Party Service Provider's operating systems must be limited to those individuals required to support the system. Third-Party Service Provider will implement appropriate change management processes. Servers and workstations will have enabled with auto-locking (password- protected) screensavers that activate after a period of inactivity. Installation of personal software is not allowed.

Third-Party Service Provider will also have mechanisms to prevent the unauthorized removal of Protected Data from the Third-Party Service Provider's networks via technologies such as removable media devices, the internet, email or instant messaging services.

Third-Party Service Provider shall ensure that only authorized devices are permitted to connect to its network. Usage of mobile devices such as cell phones and tablets must be controlled with mobile device management ("**MDM**") solutions that enable data loss prevention, data encryption and secure remote wiping of controlled devices.

4.2.2 PATCH AND VULNERABILITY MANAGEMENT. Third-Party Service Provider must analyze, test, review and subsequently install software updates on Third-Party Service Provider systems and security patches as soon as reasonably possible after release. Critical security updates must be promptly installed after testing is completed. Third-Party Service Provider will perform vulnerability scans, including scans on application and internal/external network infrastructure. Ethical hacking/penetration tests shall be performed by Third-Party Service Provider on a periodic basis. Third-Party Service Provider must review, prioritize and remediate known vulnerabilities based on identified risk factors.

4.2.3 PENETRATION TESTS. Third-Party Service Provider must conduct penetration testing and security evaluation at least annually in accordance with its Information Security Policies, which includes tests to detect vulnerabilities listed in the SANS Top-20 or Open Web Application Security Project 'OWASP' Top 10 or its successor current at the time of the penetration test and security evaluation. Third-Party Service Provider will send FIS annually (or at such other more frequent intervals as requested by FIS and mutually agreed upon by both parties) a summary of the penetration test and security evaluation to FIS. Personnel performing the penetration test must be independent of the controls being tested and do not report to the individuals who make the funding decisions for any noted vulnerabilities that require remediation. Third-Party Service Provider will (at its own cost) remediate any findings in accordance with FIS remediation timeframe policy

4.2.4 VULNERABILITY ASSESSMENT, REPORTING AND REMEDIATION OF FINDINGS.

(a) ASSESSMENT. Third-Party Service Provider must maintain a vulnerability management program based on industry standard practices that frequently assesses all Third-Party Service Provider computing devices and systems (including without limitation all such devices and systems used by Third-Party Service Provider to provide any Services under the Agreement) and all Software provided by Third-Party Service Provider under the Agreement to verify that the applicable security controls are sound, and that mitigates or eliminates vulnerabilities. As part of such program, (i) Third-Party Service Provider must use an industry standard tool to perform all vulnerability scans or engage, at its expense, an unrelated security firm to perform the assessment; and (ii) routine network, system, and software scans are scheduled on a periodic basis.

Network vulnerability scans should be performed at the following frequency, at minimum:

- External scanning: Weekly; and
- Internal scanning: at least monthly.

Internal vulnerability scanning should be performed in an authenticated state with administrator-level credentials, where technically feasible.

(b) REPORTING AND REMEDIATION OF FINDINGS. Third-Party Service Provider will send FIS annually (or at such other more frequent intervals as requested by FIS and mutually agreed upon by both parties) a summary that describes the results of the assessment. Third-Party Service Provider will (at its own cost) remediate any findings as of the result of the assessments in Sections 4.2.3 and 4.2.4.1 in accordance with FIS remediation timeframe policy.

4.2.5 ENCRYPTION. Third-Party Service Provider must have encryption and key management policies and procedures in accordance with leading information security industry standards (e.g., NIST, PCI DSS) where in-scope data is stored, processed or transmitted. The encryption algorithm should be implemented correctly and by properly maintained software without known vulnerabilities. The encryption keys can be retained by FIS or by an entity entrusted by FIS in the European Economic Area. Third-Party Service Provider will implement and operate application-level encryption ("**ALE**") technologies to protect Protected Data at rest if required by Law or, if not required by Law, within a commercially reasonable timeframe aligned with leading information security industry practices. ALE is defined as i) the encryption of in-scope data by the application ii) encryption must occur before being written to a data store or being consumed by the application,

iii) encryption must not be dependent on any underlying transport and/or other at-rest encryption including but not limited to the Third-Party Service Provider's use of native cloud encryption technologies and iv) ALE algorithms must meet strong encryption technologies (in line with industry standards such as NIST approved). Third-Party Service Provider will not transmit any unencrypted Protected Data over the internet.

4.3 CONTROL APPLICABILITY. The following requirement is only applicable if Third-Party Service Provider is (a) storing or processing Protected Data on its network, or (b) providing FIS with a Service or Software that FIS relies upon to deliver FIS' solutions to its Clients.

Third-Party Service Provider will establish and maintain disaster recovery and business continuity plans, including off-site data storage and recovery infrastructure, designed to minimize the risks associated with a disaster affecting Third-Party Service Provider's ability to provide the Services. Third-Party Service Provider's recovery time objective ("**RTO**") and recovery point objective ("**RPO**") for the Services under such plan shall conform with that set forth in the applicable Agreement or Engagement Document, or as provided to FIS in writing. Third-Party Service Provider will maintain adequate backup procedures in order to recover FIS' Data or if applicable any Client's data to the point of the last available good backup Third-Party Service Provider will test its disaster recovery and business continuity plans, including call trees, not less frequently than annually, and will provide to FIS its annual disaster recovery and business continuity plans test results. If Third-Party Service Provider fails to meet the RTO and RPO in any annual test, Third-Party Service Provider shall perform a root cause analysis of the cause of the failure to meet the RTO or RPO and will remediate the cause of such failure and retest within six (6) months of the failed test. If Third-Party Service Provider fails to meet the RTO or RPO in the retest, Third-Party Service Provider will have a second six (6) month period to remediate and retest. If Third-Party Service Provider fails a second time, FIS may request that the parties attempt to reach a mutually agreeable resolution, and if the parties are unable to agree upon a resolution within thirty (30) days of FIS' request, FIS may terminate the Agreement with no further financial obligation to Third-Party Service Provider. Third-Party Service Provider will provide its test results to FIS not later than thirty (30) days following each applicable test or retest, and agrees FIS may share such disaster recovery plan and any test results with FIS' auditors, FIS' regulators, and any Clients who have contracted for the Services. Third-Party Service Provider will implement the applicable disaster recovery or business continuity plan upon the occurrence of a disaster, and shall notify FIS promptly of such occurrence. In the event of a disaster (as defined in the plan), Third-Party Service Provider will not charge fees higher than or in addition to the agreed fees under the Agreement. Third-Party Service Provider will notify FIS of, and invite it to participate in each disaster recovery and business continuity plan test, at no additional charge to FIS.

4.4 CONTROL APPLICABILITY. The following requirement is only applicable if Third-Party Service Provider (a) stores, processes, or transmits Payment Card Data in connection with the Services under the Agreement, or (b) is otherwise subject to PCI DSS.

Third-Party Service Provider must ensure internal and external auditors regularly review its information security practices. Third-Party Service Provider will comply with the Payment Card Industry Data Security Standard requirements (as amended from time to time) ("**PCI DSS**"). In addition, (i) Third-Party Service Provider will submit their Attestation of Compliance ("**AOC**") and Vendor Responsibility Matrix within ten (10) days of the execution of the Agreement and will have an AOC and Vendor Responsibility Matrix prepared, and provide to FIS such updated AOC and Vendor Responsibility Matrix, annually thereafter; (ii) Third-Party Service Provider will publish to 'Visa' Global Service Third-Party Service Provider registry and maintain 'Green Status' in such registry throughout the duration of the Term of the Agreement; and (iii) if Third-Party Service Provider fails to maintain 'Green Status' in the Visa Global Service Third-Party Service Provider registry, the following provisions shall apply: (A) if Third-Party Service Provider in in 'Yellow Status' in the Visa Global Service Third-Party Service Provider registry, Third-Party Service Provider will provide the Services free of charge until Third-Party Service Provider obtains 'Green Status'; and (B) if Third-Party Service Provider is in 'Red Status' or is not listed in the Visa Global Service Third-Party Service Provider registry: (1) Third-Party Service Provider will provide the Services free of charge free of charge until Third-Party Service Provider obtains 'Green Status' or the Agreement terminates, (2) Third-Party Service Provider will refund to FIS the six (6) then most recent months of fees paid by FIS under the Agreement (excluding any period in which Third-Party Service Provider was providing the Services free of charge due to Third-Party Service Provider being in 'Yellow Status' or 'Red Status' pursuant to this provision), and (3) FIS may, in addition to any other remedies FIS may have, terminate the Agreement with no financial obligation to Third-Party Service Provider arising from such termination.