Proskauer

[EXHIBIT A]

Data Protection and Security

1. Definitions.

"***Proskauer***" means each of [Proskauer Rose (UK) LLP, Proskauer Rose LLP, 374 rue Saint-Honoré 75001 Paris, France, Proskauer Rose LLP (USA), Brazil, China, Hong Kong].

"***Client***" means a Person that does or has done business with Proskauer.

"***Person***" means an individual natural person, a partnership, a corporation, a limited liability company, an association, a joint stock company, a trust, a joint venture, an unincorporated organization, a governmental entity or any other entity.

"***Personal Information***" means any personally identifiable information about Proskauer's former, prospective and current employees, other personnel, agents, Clients, contractors, managers, suppliers, and/or other natural persons, and family members of the foregoing, which information may include without limitation name, address, other contact information, financial account information, insurance information, social security number or social insurance number, tax ID number, driver's license or non-driver identification card number, passport information, government ID number, tribal ID number, mother's maiden name, date of birth, password, PIN number, access code, routing code, security code, medical or medical insurance information, DNA profile information, biometrics, electronic signature or serial number, employee ID number, payroll records, salary information or other human resources records and information, "non-public information" as defined by the Gramm-Leach-Bliley Act, "protected health information" as defined by Health Insurance Portability and Accountability Act of 1996, consumer report information, alien registration number or naturalization number, personal identification number or code, or other account information and/or account activity information, other information or data that can be used for identity theft (including that which is not personally identifiable), other sensitive information regarding such natural persons and any information derived or otherwise created by Vendor in connection therewith.

"***Proprietary Information***" means proprietary information relating to Proskauer or Clients and their businesses or assets that is not generally known to the public, whether of a technical, business or other nature, including, without limitation, tax ID number, financial account information, and [ ].

"***Protected Information***" means, collectively, Personal Information and Proprietary Information.

"***Purpose***" means [insert subject matter, nature and purpose for which Vendor is permitted to use the Personal Information].

"***Special Data***" means Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data that can uniquely identify a natural person, health data, data about a natural person's sex life or sexual orientation, criminal convictions or offenses.

2. Confidentiality. Notwithstanding anything to the contrary, as between Proskauer and Vendor, all Protected Information is and shall remain the sole and exclusive property of Proskauer, and shall be deemed Proskauer's confidential information pursuant to the terms of any confidentiality agreement or non-disclosure agreement between the parties (a) regardless of whether it is marked as such, (b) regardless of whether it falls into the carve-outs from confidential information set forth in any such agreement between the parties, and (c) regardless of whether Vendor receives it directly from Proskauer or from its personnel, Client, or any of their designees or intermediaries. Additionally, any account passwords issued to Vendor or its agents for purposes of accessing Proskauer's or its systems shall be protected as if they were Protected Information for all purposes.

3. Applicable Privacy and Data Security Laws. For purposes of this **Exhibit A**, "***Applicable Privacy and Data Security Laws***" means: (a) all privacy, security, data protection and communications laws, rules and regulations of any applicable jurisdiction (including, without limitation, the U.S., Europe and each jurisdiction where a data subject resides or is located) that apply to Vendor, to Proskauer or to the Protected Information, and all then-current industry standards, guidelines and practices with respect to privacy, security, data protection, direct marketing, consumer protection and workplace privacy, including the collection, processing, storage, protection and disclosure of Protected Information, (b) the applicable data security and privacy policies of Vendor, and (c) the applicable data security and privacy policies of Proskauer that are provided by Proskauer to Vendor.

4. Limited Use and Disclosure; Compliance. Vendor agrees that, at all times during the term of the Agreement and thereafter, (a) it will comply with all Applicable Privacy and Data Security Laws in relation to Protected Information, (b) it will cooperate with Proskauer with respect to Proskauer's obligations under Applicable Privacy and Data Security Laws including without limitation by facilitating the exercise of any data subject's right to access, correct, complete, receive copies of, or erase Personal Information of such data subject, or to opt out of direct marketing, profiling, automated decision-making, or other processing, within the time frames required by Applicable Privacy and Data Security Laws, (c) Protected Information will not be utilized, accessed, stored, processed or transmitted by Vendor or its subcontractors and agents for any purpose other than as necessary for the Purpose, and only in accordance with the documented instructions of Proskauer (and not, for example and without limitation, to otherwise market to or contact such Persons, or to engage de-identification, anonymization, in data mining, analytics, marketing or any other activity outside the direction of Proskauer), (d) it must promptly notify Proskauer if, in its opinion, compliance with any Applicable Privacy and Data Security Laws may adversely affect its performance under the Agreement or may conflict with any instruction of Proskauer, and (e) it will promptly notify Proskauer in writing if it determines that it has not complied

with or is unable to satisfy any of its obligations under this **Exhibit A**. Neither Vendor nor its subcontractors and agents shall, or shall attempt to, re-identify Protected Information that has been provided to Vendor or its subcontractors and agents in a de-identified form. Vendor shall not process Special Data. Without limiting the foregoing, Vendor shall not disclose (and not allow any of its personnel, contractors or permitted agents or representatives to disclose) in any manner whatsoever any Protected Information to any third party without the prior written consent of Proskauer, except as expressly set out herein. [Vendor shall not collect any Personal Information from or about individuals except that which is actively and knowingly provided by such individuals or provided by Proskauer to Vendor.]

5. Security Measures.

(a) Without limiting Vendor's other obligations under this **Exhibit A**, Vendor shall implement and maintain a comprehensive and effective written information and data security program and reasonable security practices and procedures appropriate to the nature of the Protected Information, which policies, practices and procedures shall: (i) comply with all Applicable Privacy and Data Security Laws; (ii) include appropriate administrative, technical, organizational and physical safeguards to identify, assess and protect against any reasonably foreseeable anticipated or actual threats or hazards (whether internal or external) to the security or integrity of Protected Information, and against the loss, unavailability, destruction, theft, unauthorized access, use, alteration, disclosure or other processing of Protected Information or other breach of security safeguards, whether such Protected Information is contained in electronic, paper or other records; (iii) include: training and security awareness programs for personnel and contractors who have access to Protected Information, monitoring personnel and contractor compliance with policies and procedures, requiring personnel and contractors to agree, in writing, to protect the confidentiality and security of the Protected Information in accordance with the terms of this **Exhibit A**, appropriately screening each personnel and contractor to confirm suitability of the performance of their duties in connection with the Agreement, imposing disciplinary measures for violations of such policies and procedures, and preventing terminated employees from accessing records containing Protected Information; (iv) designate one employee to be in charge of Vendor's information security program and designate an individual to be responsible for the Vendor's compliance with this **Exhibit A** and Applicable Privacy and Data Security Laws; (v) impose reasonable restrictions on access to records containing Protected Information, make it only accessible to personnel on a need-to-know basis, and require physical and hardware media containing such records to be stored in locked facilities, storage areas or containers with need-to-know access only; (vi) design and implement information safeguards to control the risks Vendor identifies through risk assessment, regular testing, or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures to confirm the information security program is operating in a manner that is reasonably calculated to prevent and detect unauthorized access to or use or disclosure of Protected Information; and (vii) include a risk assessment of the sufficiency of any safeguards in place to control the risks described above and review the scope of security measures at least annually and when a material change in business

practices that may reasonably implicate the security or integrity of records containing Protected Information.

(b) Vendor shall: (i) use adequate user authentication protocols to prevent unauthorized individuals from accessing accounts (including multi-factor authentication to access Protected Information), and otherwise ensure Protected Information is physically or logically segregated from any other information owned or managed by Vendor or other third parties, including a reasonably secure method of assigning, selecting and controlling passwords or identifiers, restricting access to active user accounts only and blocking access to user identification after multiple unsuccessful attempts to gain access; (ii) install up-to-date firewall protection and operating system and other software security patches; (iii) install and use up-to-date system security software, including malware protections, patches and virus definitions, which is set to receive and install the most current security updates on a regular basis; (iv) log access to Protected Information, including, at a minimum, the identity of the user, time, and IP address and monitor and audit such logging; (v) encrypt all transmitted records and files containing Protected Information that will travel across public networks or be transmitted wirelessly using industry standard encryption levels; (vi) encrypt all Protected Information stored on laptops or other portable devices or stored on computing equipment that is connected to the Internet using industry standard encryption levels; (vii) prohibit its personnel from transmitting Protected Information to, or accessing Protected Information from, computers, accounts or devices not controlled by Vendor and from bringing, transporting, or transmitting Protected Information to their homes, personal computers, accounts, devices or media, other than using corporate-approved VPN terminal-only access; (viii) use reasonable measures to detect breaches of Protected Information, and maintain and train applicable personnel on policies and procedures to escalate any such detected breaches to the attention of the Vendor's executives, and (ix) adopt up-to-date and leading edge technologies in consultation with, or otherwise at the request of, Proskauer for the safe, secure and accurate collection, processing, storage, and distribution of Protected Information.

(c) Proskauer reserves the right to review, upon request, the Vendor policies, procedures and practices used to maintain the privacy, security and confidentiality of Protected Information.

(d) Each year during the Term (and during the year following the Term in respect of the last year of the Term), Vendor shall engage, at its sole cost and expense, an external auditor reasonably acceptable to Proskauer to conduct a SOC 1 Type II audit and a SOC 2 Type II audit (or any successor audit standards thereto) of Vendor's internal controls related to the provision of the applicable Services to Proskauer under the Agreement. Vendor shall deliver a copy of each report resulting from such audits to Proskauer promptly, but not later than ten (10) business days after completion thereof. In the event an audit report identifies any material deficiencies in Vendor's internal controls, Vendor shall promptly remedy such deficiencies. Notwithstanding the foregoing, Proskauer shall have the right to terminate the Agreement by providing Vendor written notice within

thirty (30) days of its receipt of the report identifying such deficiency, in which case Proskauer shall receive a pro rata refund of amounts paid under the Agreement.

(e) Promptly upon Proskauer's written request, no more than once per calendar year during the Term, Vendor shall engage, at its sole cost and expense, an external auditor reasonably acceptable to Proskauer to conduct an audit of Vendor's and its agents' and subcontractors' information technology and information security systems and procedures to verify compliance with ISO/IEC 270001:2013 Information technology – Security techniques – Information security management systems – Requirements (or any successor standards thereto) and Vendor shall deliver a copy of each such audit report to Proskauer promptly, not later than ten (10) business days after completion thereof. In the event such audit reveals that Vendor does not comply with the foregoing information security standard, Vendor shall promptly remedy such non-compliance. Notwithstanding the foregoing, Proskauer shall have the right to terminate the Agreement by providing Vendor written notice within thirty (30) days of its receipt of the report identifying such non-compliance, in which case Proskauer shall receive a pro rata refund of amounts paid under the Agreement.

(f) Without limiting the foregoing, Vendor shall provide Proskauer (or its representatives) with access to the records, facilities and premises of Vendor for the purposes of auditing, inspecting, examining and otherwise verifying Vendor's compliance with the terms of this **Exhibit A**, and in the event that any such audit, inspection or examination reveals that Vendor is non-compliant with its obligations under this **Exhibit A**, to promptly remedy such non-compliance and pay the reasonable costs associated with the audit, inspection or examination. Notwithstanding the foregoing, Proskauer shall have the right to terminate the Agreement by providing Vendor written notice within thirty (30) days of the audit, inspection or examination identifying such deficiency, in which case Proskauer shall receive a pro rata refund of amounts paid under the Agreement.

6. Notification of Security Breach and Incident Response.

(a) Without limitation of the foregoing, Vendor shall advise Proskauer promptly, without undue delay, and within twenty four (24) hours, in the event that it learns or has reason to believe that there has been a loss, theft or unauthorized access to, risk to, or use or disclosure of, or any security breach relating to or affecting Protected Information, or that any Person who has had access to Protected Information has violated or intends to violate the terms of the Agreement or this **Exhibit A**. Vendor shall, at its own expense, promptly report to Proskauer, in writing, the nature and amount or records of the Protected Information affected and the number, identity and contact information of data subjects about whom Personal Information was affected, and cooperate with Proskauer in investigating and responding to the foregoing, notifying affected individuals as required by law, and seeking injunctive or other equitable relief against any such Person or Persons who have violated or attempted to violate the security of Protected Information.

(b) Promptly upon learning of actual or suspected unauthorized access to or use of, or any security breach relating to or affecting Protected Information that is or was stored on or accessible through a computer, server, or other equipment under Vendor's or its agent's or subcontractor's responsibility, Vendor shall, at its expense, retain a nationally recognized forensics expert approved by Proskauer in writing to recommend to Vendor all steps necessary to stop any ongoing unauthorized access to such Personal Information, to preserve all records and information related to such activities and to investigate the nature and scope of the incident. Vendor shall take all steps recommended by such expert.

(c) Except as otherwise required by applicable law, Vendor will not inform any third party of any security incident involving Protected Information without first obtaining Proskauer's prior written consent (in its sole discretion). In the event that applicable law or contract requires that any Clients or other affected Persons be notified of a security incident involving Protected Information, Proskauer shall have the discretion of determining whether such notice shall come from Proskauer or Vendor, subject to applicable law. In any event, the content, timing and other details of such notice shall be subject to Proskauer's prior written approval, in Proskauer's sole discretion. Vendor shall be responsible for reimbursing Proskauer for the costs of such notifications and of fielding feedback and questions from those notified, and any other associated costs that Proskauer may incur in connection with responding to or managing the breach of the security of Protected Information, including, for example, without limitation, costs of print shop services, postage, obtaining contact information for affected individuals, credit monitoring services, call center services and forensics services.

(d) The remedies set forth herein shall be in addition to any other remedies available to Proskauer at law or in equity, including but not limited to Vendor's indemnification obligations set forth in Section 9 below.

7. Access and Disposal.

(a) Promptly upon Proskauer's request, Vendor shall provide Proskauer with access to or delivery of the Protected Information, or any portion thereof identified by Proskauer, being stored, processed or transmitted or otherwise in Vendor's possession or control or that of its agent or contractor, in a structured, commonly used, machine readable, non-proprietary format.

(b) Vendor shall retain Personal Information only until Vendor no longer needs to retain it in order to fulfill the Purpose. As soon as possible after any Protected Information (or a portion thereof) is no longer needed by Vendor to fulfill its obligations hereunder, and in any event upon termination of the Agreement for any reason, but subject to any records retention requirements instructed by Proskauer : (i) each and every original and copy in every media of such Protected Information in Vendor's possession or control shall be returned to Proskauer by Vendor, or at Proskauer's request destroyed (including without limitation, with respect to any hard copy, micro-cut shredded), (ii) all electronic copies of the Protected Information in Vendor's possession or control shall be

deleted in a manner that makes the Protected Information non-readable and non-retrievable, and (iii) Vendor will certify to Proskauer, in writing, that Vendor has complied with its obligations under this Section 7. Upon disposal under any circumstances, unencrypted Protected Information contained in print or electronic media is required to be securely shredded, destroyed, or modified so that it is unreadable and irretrievable. In the event applicable law does not permit Vendor to comply with the delivery or destruction of the Protected Information, Vendor warrants that it shall ensure the strict confidentiality of the Protected Information and that it shall not use, disclose or otherwise process any Protected Information after termination of the Agreement.

(c) If Vendor should receive any legal request or process in any form seeking disclosure of, or if Vendor should be advised by counsel of any obligation to disclose, Protected Information, Vendor shall (to the maximum extent allowed by applicable law) provide Proskauer with prompt prior notice of such request or advice so that Proskauer may seek a protective order or pursue other appropriate remedies to protect the confidentiality of such information. Vendor shall promptly comply and fully co-operate with all instructions of Proskauer with respect to any action taken with respect to such request or disclosure. Vendor agrees to furnish only that portion of the information which is legally required to be furnished and, in consultation with Proskauer, to use all reasonable efforts to assure that the information is maintained in confidence by the party to whom it is furnished.

(d) [To the extent that Vendor acts as a data controller in relation to the Personal Information (i.e. determining the means or purposes of processing the Personal Information) in accordance with the Applicable Privacy and Data Security Laws, and not just as a data processor, Vendor shall comply with the Applicable Privacy and Data Security Laws as a data controller. For the avoidance of doubt, Vendor acts as a data controller with respect to the Personal Information when it is conducting activity required to comply with know your client checks for anti-money laundering purposes and conducting sanctions screening, reporting suspicious transactions, and any request made by any financial services regulator or other public authority or governmental body having jurisdiction over Vendor.]

(e) Vendor shall immediately notify Proskauer in writing of any enquiry received by Vendor from an individual relating to, among other things, the individual's right to access, modify or correct Personal Information and any complaint received by Vendor relating to the processing of Personal Information, and promptly comply and fully co-operate with all instructions of Proskauer with respect to any action taken with respect to such enquiry or complaint.

8. Data Location; Transfer; Export.

(a) A list of locations (the "***Approved Locations***") in which Protected Information may be stored, processed, transmitted or accessed by Vendor or its subcontractors or agents in connection with provision of the Services is attached as Schedule 8(a) hereto. All Approved Locations must be within the United States, the

European Economic Area or Canada. Protected Information shall not be stored, processed, transmitted or accessed outside of the Approved Locations.

(b) Vendor shall not move Protected Information from the Approved Locations, unless required to comply with the requirements of a governmental or regulatory body (including subpoenas or court orders). Vendor further agrees (i) to notify Proskauer in writing as far as possible (and no less than fifteen (15) days) in advance of any such change in location and the legal requirement for such change, (ii) to provide Proskauer with a reasonable opportunity to challenge such requirement and protect the Protected Information and Proskauer's legal rights, and (iii) to cooperate with and comply with all instructions of Proskauer in such efforts.

(c) Vendor will take all other actions required to legitimize the transfer, including, without limitation, (i) co-operating to register the Standard Contractual Clauses with any supervisory authority in any European Economic Area country; (ii) procuring approval from any such supervisory authority; or (iii) providing additional information about the transfer to such supervisory authority. [Vendor hereby agrees to enter into the Standard Contractual Clauses for Data Processors established in Third Countries as set forth in Commission Decision 2010/87/EU, 2010 O.J. (L 39) 5-6, 11 (EU), covering any and all Personal Information contained in the Protected Information.]

9. Indemnification. Without limitation of the indemnification obligations set forth in the Agreement, Vendor hereby agrees to indemnify, defend and hold harmless Proskauer and its and their Clients, employees and agents, from and against any and all third party claims, actions, suits, or proceedings, whether civil, criminal, administrative, or investigative, including any liabilities, obligations, losses, damages, costs, fees, penalties, fines, assessments, settlements, charges or other expenses of any kind (including, but not limited to, reasonable attorneys' fees and legal costs) arising from any third party claims (collectively, "***Claims***"), including without limitation actions or investigations (formal or informal) by regulatory bodies, authorities or agencies and private Claims, where such Claims arise out of Vendor's or its agent's or subcontractor's non-conformance with this **Exhibit A** or a Security Event (as defined below). For purposes of this Section 9, a "***Security Event***" is an event where Protected Information that was under Vendor's or its agent's or subcontractor's responsibility or possession is stolen, lost, accessed, received, used or disclosed otherwise processed by a Person who is not authorized to access, receive, use, disclose or otherwise process such Protected Information. Proskauer expressly reserves the sole right, at Proskauer's option, to control the defense and/or settlement of any such Claim and, in such event, in addition to Vendor's other obligations in this Section 9, Vendor agrees to assist Proskauer, at Vendor's expense, in the defense of any such Claim.

10. Insurance.

Throughout the term of the Agreement and any renewals thereof, Vendor shall maintain, at its own expense, the insurance coverage listed on Schedule 10, as well as any insurance normally maintained by reasonable entities in the industry.

11. Agents and Subcontractors.

(a) Vendor acknowledges and agrees that no subcontractor or agent of Vendor is permitted to have access or exposure to Protected Information, except for those subcontractors or agents set forth on Schedule 11(a), which may, pursuant only to Proskauer's express prior written consent, be amended from time to time by Vendor. Before allowing or enabling a subcontractor or agent to have access to Protected Information, Vendor shall evaluate and validate the subcontractor's or agent's capabilities to maintain the security of Protected Information in accordance with this **Exhibit A**. Vendor represents and warrants that Schedule 11(a) sets forth a complete and accurate list of all of Vendor's subcontractors and agents permitted to have access or exposure to Protected Information. Notwithstanding the foregoing, Proskauer shall have the right to terminate the Agreement by providing Vendor written notice within thirty (30) days of its receipt of a proposed amendment to Schedule 11(a) to which Proskauer objects due to a suspected or actual security deficiency with respect to any subcontractor or agent, in which case Proskauer shall receive a pro rata refund of amounts paid under the Agreement.

(b) Subject to Section 11(a), to the extent that Vendor engages any subcontractor or agent to perform services under the Agreement and such subcontractor or agent has access to any Protected Information, Vendor shall contractually require each such subcontractor or agent to comply with all of Vendor's obligations with respect to Protected Information as set forth in Sections 2, 3, 4, 5, 6, 7, 8, 10 and 11 of this **Exhibit A** as if such subcontractor or agent were Vendor, and Vendor agrees that, notwithstanding anything to the contrary in any agreement between Vendor and Proskauer, Vendor shall remain fully and primarily liable for any liability arising from or relating to the acts or omissions of such subcontractor or agent with respect to Protected Information. For the avoidance of doubt, Vendor shall maintain control over all Protected Information it entrusts to any subcontractor or agent (and all such Protected Information shall be deemed under Vendor's control for purposes hereunder), and the right of such subcontractor or agent to process any Protected Information shall terminate automatically upon termination of the Agreement for any reason.

12. Limitation of Liability. Vendor's limitations and disclaimers of liability set forth in any other agreement between the parties shall not apply to liability arising from its or its agents' or subcontractors' non-conformance with this **Exhibit A**, or from a Security Event arising from Vendor's or its agent's or subcontractor's negligent act or omission. [**Optional Addition:** Vendor's liability arising from its or its agent's or subcontractor's non-conformance with this **Exhibit A** or from a Security Event shall not exceed the greater of: (a) its insurance coverage of same [pro-rated among its affected customers], provided that such insurance coverage meets the requirements of Section 10 and Schedule 10 of this **Exhibit A**, and (b) [$TBD]. **[Note: Appropriate number to be inserted depending on the amount and nature of the data Vendor will be handling.]**

13. Vendor's duties under this **Exhibit A** shall be fulfilled at Vendor's own expense with no cost to Proskauer. Notwithstanding anything to the contrary, this **Exhibit A** shall survive termination or expiration of the Agreement.

14. In the case of conflict or ambiguity between: (a) any provision contained in the body of this **Exhibit A** and the provisions of the Agreement, the provisions of this **Exhibit A** will prevail; and (b) any of the provisions of this **Exhibit A** or the Agreement and any Standard Contractual Clauses executed by the parties, the provisions of such Standard Contractual Clauses will prevail.

Schedule 8(a)

Approved Locations

Schedule 10

Insurance

Cyber Risk and Privacy Insurance ("***Cyber Insurance***") issued by one or more insurers with a minimum A.M. Best Financial Strength rating of "A- (Excellent) VIII", written on forms of policies satisfactory to Proskauer, and covering third-party liability, loss or damage arising from or related to any act, error, omission, negligence, misrepresentation or breach of duty arising from or relating to, performance or breach of Vendor's obligations under the Agreement, including but not limited to any:

- privacy or security breach;
- use, theft or release of data, confidential information (including personally identifiable information),
- unauthorized use, access or tampering with network or computer systems, including hacker attacks;
- loss to or destruction of data, network or computer systems, including introduction of a computer virus, malware, ransomware or key-logger into or otherwise causing damage to a computer, computer system, network or similar computer-related property, data or software;
- ID theft;
- business income loss;
- cyber extortion attack or threat;
- electronic or computer crime;
- media liability; and
- internet liability.

Such Cyber Insurance may be provided by one or more coverage parts of Vendor's package errors and omissions ("***E&O***") policy; provided, however, that the limits of liability available for such Cyber Insurance shall be no less than $[TBD] **[Note: Appropriate number to be inserted depending on the amount and nature of the data**

Vendor will be handling.] per claim, event or occurrence, and contain no sublimits. Any retentions or deductibles shall be no greater than $25,000 per claim, event or occurrence, and any/all retentions and deductibles shall be the sole responsibility of Vendor and shall not apply to Proskauer. With respect to liability coverage, the Cyber Insurance shall include a five (5) year extended reporting period from the date of termination of the Agreement or any renewals thereof. Such Cyber Insurance shall also include a waiver of subrogation against Proskauer, and shall be expressly primary to any coverage maintained by Proskauer. Proskauer shall be named as an additional insured party under such insurance with respect to any liability, loss or damage arising from or relating to the Agreement. Such Cyber Insurance policy(ies) must contain Cross Liability Endorsements, or their equivalents, preserving coverage for suits by one insured against another insured. Vendor shall deliver copies of policies and certificates of insurance to Proskauer prior to the commencement of the Agreement and thereafter upon Proskauer's request. Each such certificate shall (a) indicate that policies providing coverage and limits of insurance are in full force and effect, and (b) provide that no less than thirty (30) days' written notice shall be given to Proskauer prior to cancellation, termination, or material alteration of any one of the policies. In the event of any change in policy form or carrier at renewal, Vendor shall deliver copies of the form of the policies to Proskauer at least two weeks prior to inception. Within ten (10) days after the renewal of any insurance policy required hereunder, Vendor shall deliver to Proskauer a certificate of insurance attesting to the renewal of such insurance. Nothing in this Schedule shall be deemed to limit Vendor's liability to the coverage amounts stated herein.

Schedule 11(a)

Subcontractors and Agents of Vendor