DATA PROCESSING ADDENDUM
RSA TO PROVIDER

"**Effective Date**"	
"**RSA**"	RSA Security LLC and its applicable Affiliates
"**RSA Notice Address**"	RSA Security LLC Attn: Legal Dept 174 Middlesex Turnpike Bedford MA 01730 *With a copy to:* legalnotices@rsa.com
"**Provider**"	_____[*Name*], a _____ [*Type of Entity*]. This Agreement shall apply to Provider, the corporate parent of Provider, if any, and any Affiliate of Provider or of its corporate parent that are providing Solutions.
"**Provider Notice Address**"	
"**Provider Agreement**"	_____Agreement dated _____[*Effective Date of Agreement*] between _____ [*Provider party*] and _____ [RSA *party*] together with any other agreements between RSA and Provider pursuant to which RSA is purchasing Solutions.

This Data Processing Addendum and the Standard Contractual Clauses are hereby acknowledged and agreed by each party's authorized representative and made a part of this Agreement.

RSA SECURITY LLC

By: _____

Name: _____

Title: _____

Date: _____

PROVIDER

By: _____

Name: _____

Title: _____

Date: _____

RSA and Provider have entered into a Provider Agreement under which Provider may Process RSA Data in connection with the provision of Solutions. This Data Processing Addendum ("DPA") governs Provider's Processing of RSA Data and shall form part of and be incorporated by reference into the Provider Agreement. At all times during the term of the Provider Agreement, or after the term if Provider retains access to RSA Data, Provider shall, and shall cause its Representatives and Subprocessors to, comply with this DPA. In the event of a conflict between the DPA and the Provider Agreement, this DPA shall prevail.

1. **DEFINITIONS.** Terms not defined herein have the meanings set forth in the Provider Agreement.

1.1 "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with another entity. For purposes of this definition, "control" means direct or indirect ownership or control of more than 50% of the voting interests of the entity.

1.2 "**Data Breach"** means any accidental, unlawful, or unauthorized destruction, alteration, disclosure, or access to RSA Data or any act or omission that compromises or undermines the physical, technical, or organizational safeguards put in place by Provider in Processing RSA Data or otherwise providing Solutions.

1.3 "**Controller**" means an entity which, alone or jointly with others, determines the purposes and means of the Processing of the Personal Data.

1.4 "**Processor**" means an entity which Processes the Personal Data on behalf of the Controller in order to perform Solutions purchased by RSA under the Provider Agreement, or as otherwise defined as "Service Provider" under the Privacy Laws.

1.5 "**EEA**" means the Member States of the European Union plus Norway, Iceland, and Liechtenstein.

1.6 "**GDPR**" means the General Data Protection Regulation 2016/679 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data as may be amended or superseded from time to time.

1.7 "**Highly Restricted Data**" means Social Security or other government-issued identification numbers, medical or health information, account security information, individual financial account information, credit/debit/gift or other payment card information, account passwords, individual credit and income information, intellectual property, proprietary business models, pricing, customer infrastructure/system information or data flows, and sensitive personal data as defined under Privacy Laws.

1.8 "**Personal Data**" means any information or data that alone or together with any other information relates to an identified or identifiable natural person ("**Data Subject**"), or as otherwise defined as "personal data" or "personal information" under Privacy Laws. An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, or location data.

1.9 "**Privacy Laws**" means any law, statute, directive, or regulation, including any and all legislative and/or regulatory amendments or successors thereto, regarding privacy, data protection, information security obligations, and/or the Processing of Personal Data (including the GDPR) to which a party to this DPA is subject and which are applicable to the Solutions provided.

1.10 "**Provider**" means the party from which RSA is purchasing Solutions under the Provider Agreement and its Representatives.

1.11 "**Provider Agreement**" means any agreement or agreements between RSA and Provider pursuant to which RSA is purchasing Solutions from Provider.

1.12 "**Processing**", "**Processed**", or "**Process**" means any operation or set of operations performed upon RSA Data whether or not by automated means, including access, receipt, collection, recording, organization, alteration, retrieval, retention, storage, transfer, or disclosure (including disclosure by transmission).

1.13 "**Representatives"** means any employee, officer, agent, consultant, auditor, Affiliate, Subcontractor, outsourcer, or other third party acting on behalf of Provider in connection with providing Solutions.

1.14 "**RSA Data**" means confidential information and Personal Data provided by RSA, its customers, authorized agents, and/or Subcontractors to Provider, or accessed by Provider through RSA's network and Processed by Provider in connection with the provision of Solutions, including Highly Restricted Data.

1.15 "**Solutions**" means any hardware, software (including third party components), software-as-a-service, services, or hosting services provided to RSA or an RSA customer pursuant to the Provider Agreement.

1.16 **"[EU] Standard Contractual Clauses"** are the clauses as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and located at https://ec.europa.eu/info/law/law-topic/data- protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

1.17 **"[UK] Standard Contractual Clauses"** are the International Data Transfer Addendum to the Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018.

1.18 "**Subcontractors**" means any third party acting for or on behalf of Provider, providing Solutions to RSA, or to whom Provider has assigned or delegated its contractual obligations.

1.19 **"Subprocessor"** means a third party engaged by Provider in connection with the Processing of Personal Data.

2. **ROLE OF THE PARTIES.**

2.1. The parties agree that RSA is the Controller of Personal Data and Provider is the Processor of Personal Data. When RSA acts as a Processor of Personal Data, the Provider is a Subprocessor. Provider shall not determine the purposes and means of the Processing of the Personal Data without RSA's prior agreement in writing, in which case Provider shall be deemed a Controller and shall only Process the Personal Data as agreed in writing with RSA and in full compliance with all Privacy Laws.

3. **PROVIDER OBLIGATIONS - PROCESSING OF PERSONAL DATA.**

3.1. Provider shall, in providing the Solutions, Process RSA Data in accordance with RSA's documented instructions and in compliance with Privacy Laws. Provider shall not knowingly Process any RSA Data in a manner that results in RSA being in breach of Privacy Laws, and shall immediately inform RSA, in writing at privacy@rsa.com, if in its opinion, RSA instructions infringe Privacy Laws.

3.2. RSA hereby instructs and authorizes Provider to Process RSA Data for the sole and exclusive purposes of performing Provider obligations in accordance with the Provider Agreement and other reasonable written instructions provided by RSA that are consistent with the terms of the Provider Agreement, Privacy Laws, and this DPA.

3.3. The subject matter of Processing of Personal Data, the duration of the Processing, the Data Subjects, and the categories of data, are described in Annex I to this DPA.

3.4. Provider shall ensure that its Representatives, Subcontractors, and Subprocessors engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and are under obligations of confidentiality. All RSA Data is confidential information as defined in the Provider Agreement or in a non-disclosure agreement between the parties. However, any exclusions to the definition of confidential information in such agreements shall not apply to the definition of RSA Data. Provider shall treat RSA Data as confidential information for as long as Provider has possession or control of RSA Data, including when RSA Data is held in archive, or backup or business continuity/recovery systems.

3.5. Provider shall ensure that access to Personal Data is limited to Representatives, Subcontractors, and Subprocessors who require access to provide the Solutions.

3.6. If Provider is required by Privacy Law or any other law, rule, or regulation, to disclose Personal Data (including to a government authority) or permit Processing of Personal Data by a third party, Provider shall, promptly and without undue delay, notify RSA in writing at privacy@rsa.com, and cooperate with RSA to challenge the demand and limit the extent and scope of the transfer, disclosure, or Processing.

3.7. Provider shall maintain an updated written or electronic Record of Processing Activities, as described in GDPR Article 30, describing all the activities carried out with RSA Data and Personal Data.

3.8. Provider shall cooperate and assist RSA in connection with any transfer impact assessment and privacy impact assessment which RSA may carry out in relation to the Provider's Processing of Personal Data, including any prior consultation with supervisory authorities or other competent data privacy authorities which RSA reasonably considers to be required by Privacy Laws.

3.9. Prior to Processing any payment card information in connection with a Provider Agreement, Provider must comply with, and remain in compliance with, at its expense, the Payment Card Industry Data Security Standards. Provider must submit an attestation to RSA each year stating it is current in the PCI Report on Compliance/Self-Assessment Questionnaire and PCI Quarterly Network Scan filings, and that it remains PCI-compliant. Provider shall provide any supporting documentation as reasonably required by RSA. If at any point Provider is not in compliance or is unable to or unwilling to produce adequate evidence of compliance, Provider shall be in breach of the Provider Agreement and RSA may immediately terminate the Provider Agreement and this DPA without liability to RSA.

4. **SUBPROCESSORS.**

4.1. Provider shall not transfer, sell, disclose, subcontract the Processing of, or permit the Processing of RSA Data by any Subprocessor without RSA consent. Provider shall notify RSA of a new Subprocessor by email to privacy@rsa.com, and RSA shall have fifteen (15) business days to object to the new Subprocessor. Provider shall use reasonable efforts to: (a) avoid Processing of Personal Data by the new Subprocessor, (b) make available a change in the Solution, or (c) work with RSA and the Subprocessor to ensure that the subprocessing is performed in a manner that is reasonably acceptable to RSA. If the parties cannot find a resolution within sixty (60) days, then RSA may terminate the Solutions that cannot be provided without the use of the new Subprocessor.

4.2. Provider shall have a written agreement with each Subprocessor that will Process RSA Data, which includes obligations no less protective than the obligations of this DPA (including the EU and UK Standard Contractual Clauses) and shall provide a copy of the agreement upon request.

4.3. Provider shall have sole liability for all acts or omissions of Representatives and Subprocessors.

4.4. Provider shall audit each Subprocessor that Processes RSA Data at least once every twelve (12) months, and more frequently in the event of a Data Breach. If the audit reveals any deficiencies, breaches, and/or failures by the Subprocessor, Provider shall promptly notify RSA at privacy@rsa.com. Provider shall use reasonable efforts to remedy the issue, and if, in RSA's sole discretion, a satisfactory remedy cannot be implemented within a reasonable time, RSA may instruct Provider not to use the Subprocessor, and the Subprocessor shall promptly return or delete any RSA Data in the Subprocessor's possession or control.

5. **RIGHTS OF DATA SUBJECTS.**

5.1. Provider shall, to the extent allowed by law, promptly and without undue delay, notify RSA if it receives a complaint, request, or

inquiry from a Data Subject to exercise the Data Subject's rights in relation to access, rectification, restriction of Processing, erasure, data portability, objection to Processing, or being subject to automated individual decision making. Provider shall provide all reasonable cooperation, assistance, information, and access to the Personal Data in its possession, custody, or control to allow RSA to respond to the complaint, request, or inquiry within the timeframe required by Privacy Laws. Provider shall not respond to any complaint, request, or inquiry unless instructed in writing by RSA.

6. **SECURITY AND AUDITS.**

6.1. Provider shall maintain appropriate technical and organizational measures equal or better than those described in Appendix 2 of this DPA and ensure they address the risks associated with transfers of Personal Data. Provider shall regularly monitor compliance with these measures and shall not materially decrease the overall security of the Solution for as long as Provider has Personal Data in its possession.

6.2. Provider shall make available to RSA and/or RSA's independent third-party auditor, information regarding Provider's compliance with the obligations set forth in this DPA. Provider shall permit RSA and/or its independent third-party auditor to: (a) audit Provider's compliance with this DPA, and (b) inspect any Personal Data in the custody, control, or possession of Provider. Provider shall promptly respond to all RSA inquiries with respect to Provider's handling of Personal Data.

6.3. RSA shall provide thirty (30) days' notice, in writing, prior to an on-site audit. Before the on-site audit, the parties shall mutually agree upon the scope, timing, and duration of the audit. The audit shall take place during normal business hours. RSA shall notify Provider of any non-compliance discovered during the audit, and Provider shall use commercially reasonable efforts to address the non-compliance.

7. **DATA BREACH.**

7.1. Provider shall notify RSA promptly and without undue delay at privacy@rsa.com after becoming aware of an actual or reasonably suspected Data Breach relating to Personal Data. Provider shall not inform any third party of any Data Breach without first obtaining RSA's written consent unless disclosure is required by Privacy Laws. In such case, Provider will cooperate with RSA to limit the scope to only that information which is required by Privacy Laws.

7.2. Provider shall, to the extent such information is known or available at the time, notify RSA at privacy@rsa.com of the following: (a) the nature of the Data Breach, the categories and approximate number of Data Subjects affected, and the number of Personal Data records concerned, (b) the name and contact information of the data protection officer or other point of contact, (c) a description of the likely consequences of the Data Breach, and (d) a description of the commercially reasonable measures taken or proposed to be taken by Provider to address the Data Breach. Provider may provide the information in phases if unable to provide the information at the same time.

7.3. Provider shall reimburse RSA for costs RSA incurs in responding to, remediating, and/or mitigating damages caused by Provider's Data Breach, including responding to complaints by an individual Data Subject or a regulator.

8. **RETURN OR DELETION OF PERSONAL DATA.**

8.1. Upon termination of the Provider Agreement or upon request by RSA, whichever is first, Provider shall, and ensure that its Representatives, Subcontractors, and Subprocessors immediately cease all Processing of RSA Data and return the RSA Data to RSA in a secure manner as directed by RSA, or dispose of, destroy, or render permanently anonymous all RSA Data and certify in writing that the RSA Data has been disposed of, destroyed, or rendered permanently anonymous.

8.2. If a law, rule, or regulation requires Provider to keep any RSA Data, Provider shall not use the RSA Data for any purpose other than as required by such law, rule, or regulation. Provider shall remain bound to the provisions of the Provider Agreement and any non-disclosure agreement for as long as the RSA Data is in Provider's possession or control.

9. **INTERNATIONAL TRANSFERS.**

a.1. Provider may only transfer Personal Data from the EEA and/or UK to countries outside the EEA and/or UK (which are not subject to an adequacy decision under Data Protection Laws) when the transfer is strictly necessary for the provision of the Solutions and is subject to the terms of the EU and/or UK Standard Contractual Clauses, respectively. Where the EU and/or UK Standard Contractual Clauses apply to a transfer in accordance with this Section, they are specifically incorporated into this DPA by reference and made a part hereof.

a.2. The attached Annexes I, II, and III form part of the EU Standard Contractual Clauses.

(a) Provider and RSA agree that:

1. When RSA acts as the Controller and Provider as a Processor, then Module Two applies.
   i. The appropriate designation is set forth in Annex I attached hereto.
   ii. Option 2 for Clause 9(a) applies. Provider shall inform RSA of any intended changes to sub- processors at least 60 days in advance.
   iii. Option 2 for Clause 17 applies. As described in Clause 17, Parties agree that the law of Ireland shall be the governing law.
   iv. For Clause 18, disputes shall be resolved in the courts of Ireland.
   v. Annex II and III are set below.

(b) Provider and RSA agree that, where the transfer of Personal Data from RSA to Provider in connection with the Services constitutes a transfer which is subject to the UK Standard Contractual Clauses, Provider and RSA shall comply with the UK Standard Contractual Clauses in relation to such transfer (which for these purposes are hereby incorporated into this

Agreement and executed by the parties) with the designations and amendments set out in Annex IV to this DPA.

a.3. If the EU or UK Standard Contractual Clauses cease to provide a valid legal basis for the transfer of Personal Data to countries outside the EEA or UK, the parties shall promptly meet to discuss what alternative methods are available to facilitate the transfer of the Personal Data in accordance with Privacy Laws and implement an agreed method as soon as practicable.

a.4. If Privacy Laws require that further steps be taken in relation to any applicable data export restrictions to permit the transfer of Personal Data under the Provider Agreement, including to Provider's Representatives, Subcontractors, and Subprocessors, Provider will comply with such requirements, including executing any applicable data transfer agreements to ensure that appropriate safeguards are in place for the transfer.

10. **INDEMNIFICATION.**

10.1. Provider shall defend, indemnify, and hold harmless RSA, and RSA's directors, officers, employees, Representatives, and agents from and against any and all claims, actions, demands, and legal proceedings and all liabilities, damages, losses, judgments, authorized settlements, costs, fines, penalties, and expenses, including reasonable attorneys' fees arising out of or in connection with: (a) Provider's breach of this DPA, (b) Provider's failure to comply with the Payment Card Industry Data Security Standards, and (c) violation by the Provider of any Privacy Laws.

11. **RSA AFFILIATE RIGHTS.**

11.1. Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA. Where the Solutions include the Processing by Provider Representatives, Subcontractors, or Subprocessors of RSA Data on behalf of RSA and any of its applicable Affiliates, each such Affiliate is intended to be a third-party beneficiary and may enforce the terms of this DPA as a third-party beneficiary against Provider in respect of such Affiliate's own RSA Data, as if such Affiliate were a party to this DPA and/or any Provider Agreements.

12. **MISCELLANEOUS.**

12.1. Provider's obligations under this DPA shall survive the termination or expiration of the DPA and the Provider Agreement and shall continue in effect for as long as Provider continues to possess or Process RSA Data.

12.2. Legal notices shall be made in writing to the Notice Address set forth in the Provider Agreement. Written notice made by facsimile, overnight courier, registered mail, or certified mail and sent to the RSA Notice Address or Provider Notice Address are deemed to be effective upon sending. All other written communications, deliveries, or business notices between Provider and RSA required by, permitted by, or pertaining to this DPA shall be effective when received.

12.3. Provider may not assign or transfer this DPA in whole or in part, whether voluntarily, by contract, or by merger (whether the Provider is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of RSA. Any attempt to assign or transfer this DPA other than in accordance with this Section shall be null and void. RSA may assign the DPA without Provider consent.

12.4. No waiver of any term or condition is valid unless in writing and signed by authorized representatives of both parties and shall be limited to the specific situation for which it is given. No amendment or modification to this DPA shall be valid unless set forth in writing specifically referencing this DPA and signed by authorized representatives of both parties. No other action or failure to act shall constitute a waiver of any rights.

12.5. This DPA sets forth the entire agreement and understanding of the parties relating to the subject matter herein and replaces all prior or contemporaneous discussions and agreements between the parties, both oral and written.

12.6. In performing Provider's responsibilities pursuant to this DPA, it is understood and agreed that Provider is at all times acting as an independent contractor and that Provider is not a partner, joint venturer, or employee of RSA. It is expressly agreed that Provider will not, for any purpose, be deemed to be an agent of RSA, and the parties agree to take any and all such action as may be reasonably requested by RSA to inform the public and others utilizing the professional services of Provider of such fact.

12.7. Each of the parties agrees to execute any document or documents that may be requested from time to time by the other party to implement or complete such party's obligations pursuant to this DPA or Privacy Laws. The parties agree to take such reasonable actions as are necessary to amend this DPA from time to time for RSA to comply with Privacy Laws.

12.8. Any ambiguity in this DPA will be resolved in favor of a meaning that permits RSA to comply with Privacy Laws.

12.9. The DPA and any disputes between Provider and RSA and their Representatives, including without limitation, tort and statutory claims arising under or relating in any way to the DPA or any relationships contemplated herein shall be governed and construed in accordance with the laws of the Commonwealth of Massachusetts, exclusive of any provisions of the United Nations Convention on the International Sales of Goods and without regard to its principles of conflicts of law. Provider and RSA irrevocably submit and consent to the exclusive jurisdiction and venue of the federal and state courts in the Commonwealth of Massachusetts. The parties agree that such courts shall be the exclusive proper forum for the determination of any claim or dispute arising out of, or in connection with, the DPA and waive any objection to venue or convenience of forum.

Annex I

Annex I to the EU Standard Contractual Clauses

A. **LIST OF PARTIES**

Module Selection

Select applicable Module(s)	
	Module One: Controller to Controller
X	Module Two: Controller to Processor
	Module Three: Processor to Processor
	Module Four: Processor to Controller

Data exporter(s):

Name: "RSA" as identified in the Agreement.
Address: Bays 81/82, Caherteige, Shannon, Co. Clare, Ireland or the address for RSA as specified in the Agreement.
Contact person's name, position and contact details: Data Protection Officer privacy@rsa.com
Activities relevant to the data transferred under these Clauses: The activities are specified in Section 3 of the Addendum.
Signature and date: [answer]
Role (controller/processor): Controller.

Data importer(s):

Name: [answer]
Address: [answer]
Contact person's name, position and contact details: [answer] **Activities relevant to the data transferred under these Clauses**: [answer] **Signature and date**: [answer]
Role (controller/processor): Processor.

B. **DESCRIPTION OF TRANSFER**

***Categories of data subjects whose personal data is transferred**:*
[answer]

***Categories of personal data transferred**:*
[answer]

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**:*
[answer]

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):
[answer]

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**:*
[answer]

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**:*
[answer]

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13:
Ireland

Annex II

Annex II to the EU Standard Contractual Clauses. Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

Provider takes information security seriously and this approach is followed in its Processing and transfers of Personal Data. This information security overview applies to Provider's corporate controls for safeguarding Personal Data which is Processed and transferred in accordance with the DPA.

SECURITY PRACTICES. Provider has implemented corporate information security practices and standards that are designed to safeguard its corporate environment and to address business objectives across the following areas: (1) information security, (2) system and asset management, (3) development, and (4) governance. These practices and standards are approved by the Provider's executive management and are periodically reviewed and updated where necessary. Provider shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security, and the treatment of Personal Data and sensitive personal data throughout its lifecycle. Key policies shall be reviewed at least annually, and Provider shall evaluate organizational and administrative risks no less than annually, and system and technical risks no less than quarterly.

Provider shall preserve the confidentiality, integrity and availability of RSA Data, including: (a) physical controls that restrict and monitor access to systems that Process RSA Data, (b) technical and administrative controls that protect against malicious software and malicious actors, (c) strong encryption of data in transit across untrusted and public networks and, in the case of Highly Restricted Data, at rest in all locations where it is stored, (d) periodic encryption key rotation and management, (e) prohibition of Highly Restricted Data and Personal Data being Processed in non-production environments, (f) regular security control reviews and effectiveness testing, and (vii) strong technical and administrative controls regarding remote access and mobile devices.

ORGANIZATIONAL SECURITY. It is the responsibility of the individuals across the Provider's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, Provider's Information Security ("**IS**") function is responsible for the following activities:

1. **Security strategy** – drives Provider's security direction and works to ensure compliance with security-related policies, standards, and regulations, and to raise awareness, and provide education to users. This IS function also carries out risk assessments and risk management activities and manages contract security requirements.
2. **Security engineering** – manages testing, design, and implementation of security solutions to enable adoption of security controls across the environment.
3. **Security operations** – manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.
4. **Forensic investigations** – works with security operations, legal, privacy, human resources to carry out investigations, including eDiscovery and eForensics.
5. **Security consulting and testing** – works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

APPROPRIATE SECURITY SAFEGUARDS. Provider shall Process the RSA Data in a manner that ensures appropriate security of the RSA Data (including protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage) using appropriate technical and/or organizational measures which ensure a level of security commensurate to the risk, including as appropriate:

1. The encryption of RSA Data,
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services,
3. The ability to restore the availability and access to the RSA Data in a timely manner in the event of a physical or technical incident, and
4. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of RSA Data.

In assessing the appropriate level of security, Provider shall take account of the risks that may be presented by the Processing of the RSA Data, in particular, from a Data Breach. Provider agrees to have in place and maintain as a minimum those information security measures set out in the DPA. As part of its compliance with this clause, Provider shall have and maintain appropriate and industry-standard physical, organizational, and technical processes, security standards, guidelines, controls, and procedures ("**Policies**") to protect against any Data Breach ("**Appropriate Safeguards**").

Provider shall regularly, but in no event less than annually, evaluate, test, and monitor the effectiveness of its Appropriate Safeguards and shall promptly adjust and update Appropriate Safeguards as reasonably warranted by such results. Provider shall, upon request, provide RSA with a written description of the Appropriate Safeguards. Provider shall provide RSA with access to relevant documentation and reporting on the implementation, certification, effectiveness, and remediation of the Appropriate

Safeguards. Provider represents, warrants, and covenants that Provider and its Subprocessors and Subcontractors do and shall implement and maintain similar Policies.

ASSET CLASSIFICATION AND CONTROL. Provider shall track and manage key information and physical, software, and logical assets such as:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information
- software assets, such as identified applications and system software
- physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling Personal Data provides the framework for technical, organizational, and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

Provider shall: (a) identify all equipment and media used in the Processing of RSA Data, (b) assign responsibility for all equipment and media to one or more custodians, and (c) require regular reviews of the asset inventory for accuracy and to identify missing equipment and media.

Provider shall ensure that media containing RSA Data is securely handled, including: (a) strong encryption of RSA Data on all mobile devices and removable storage, (b) requirement for secure sanitization and destruction methods for media that at any time held RSA Data, and (c) requirement that all media, including paper, containing unencrypted RSA Data be stored in a secure location.

EMPLOYEE SCREENING, TRAINING AND SECURITY

1. **Screening/background checks:** Where reasonably practicable and appropriate, as part of the employment/recruitment process, Provider shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to Provider's networks, systems, or facilities.
2. **Identification:** Provider shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other Provider Affiliates or customers for whom the employee is providing services.
3. **Training:** Provider's annual compliance training program includes a requirement for employees to complete a data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.
4. **Confidentiality:** Provider shall ensure its employees are legally bound to protect and maintain the confidentiality of any Personal Data they handle.

PHYSICAL ACCESS CONTROLS AND ENVIRONMENTAL SECURITY

1. **Physical Security Program:** Provider shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. Provider's security team shall work closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which Personal Data is Processed and continually monitor any changes to the physical infrastructure, business, and known threats. Provider's security team shall also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of RSA. Provider shall balance its approach toward security by considering elements of control that include architecture, operations, and systems.
2. **Physical Access controls:** Physical access controls/security measures at Provider's facilities/premises are designed to meet the following requirements:

   (a) Access to Provider's buildings, facilities, and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to the Provider. Only personnel associated with Provider are given access to Provider's facilities and physical resources in a manner consistent with their role and responsibilities in the organization.

   (b) Relevant Provider facilities are secured by an access control system. Access to such facilities is granted with an activated card only.

   (c) All persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g., a badge or keycard assigned to one individual) by the IS function. Individuals issued unique physical access credentials are instructed not to allow or enable other individuals to access the Provider's facilities or resources using their unique credentials (e.g., no "tailgating"). Temporary (up to fourteen (14) days) credentials may be issued to individuals who do not have active identities where this is necessary: (i) for access to a specific facility, and (ii) for valid

business needs. Unique credentials are non-transferable and if an individual cannot produce his/her credentials upon request, he/she may be denied entry to Provider's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative.

(d) Employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices, and documents in a secure location (especially while traveling), and log out or shut down their computers when away from their desk.

(e) Visitors who require access to Provider's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building, and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, Personal Data, visitors are not allowed un-escorted access to restricted or controlled areas.

(f) Select Provider facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted.

(g) Locked shred bins are provided on most sites to enable secure destruction of confidential information/Personal Data.

(h) For Provider's major data centers, security guards, UPS, and generators, and change control standards are available.

(i) For software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

CHANGE MANAGEMENT. The IT organization manages changes to the corporate infrastructure, systems, and applications through a centralized change management program, which may include testing, business impact analysis, and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

SECURITY INCIDENTS AND RESPONSE PLAN

1. **Security incident response plan:** Provider maintains a security incident response policy and related plan and procedures which address the measures that Provider will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized acquisition of Personal Data. These measures may include incident analysis, containment, response, remediation, reporting, and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the Provider's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

3. **Contingency Planning Policies:** Provider shall define roles and responsibilities and provide clear guidance and training on the proper handling of contingency events including: (a) natural threat events such as floods, tornadoes, earthquakes, hurricanes, and ice storms, (ii) accidental threat events such as chemical spills and mechanical or electrical failures, and (iii) intentional acts such as privacy and security breaches, bomb threats, assaults, and theft.

SOLUTION SECURITY

1. Vulnerabilities. Provider shall have controls in place to identify any security vulnerabilities in the Solutions during development and after release. Provider shall provide RSA written notice of: (a) publicly-acknowledged vulnerabilities/zero-day exploits within five (5) business days of the public acknowledgement, and (b) internally-known yet publicly-undisclosed vulnerabilities/zero-day exploits within ten (10) business days of their discovery. Provider commits to remediate all vulnerabilities identified in the Solutions at Provider's expense, and to remediate vulnerabilities with a base score above 4 as defined by Common Vulnerability Scoring System in a timeframe commensurate with the risk or as agreed upon with RSA. Provider's use of open source code shall not alter Provider's responsibility to identify and remediate vulnerabilities as described here.
2. Coding Practices. Provider agrees: (a) to use industry secure-coding practices (such as Microsoft's Software Development Lifecycle, Digital Software Security Touchpoints, OWASP standards or Sans Top 25), (b) the Solutions are designed based on industry secure-coding practices, and (c) information security is addressed throughout the development lifecycle. The Solutions' processes, direct capabilities, and other necessary actions shall comply with all PCI standards and Privacy Laws.
3. Security Assessments. Provider shall submit the results and remediation efforts of an independent security assessment for all Solutions that: (a) are customer facing, including websites, shipped with, or installed on customer systems, or (b) Process Highly Restricted Data. The assessment scope and remediation efforts must be agreed upon by RSA and addressed to RSA's satisfaction prior to acceptance of such Solutions.

DATA TRANSMISSION CONTROL AND ENCRYPTION. Provider shall, to the extent it has control over any electronic transmission or transfer of Personal Data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered, or removed without proper authority during its transmission or transfer. Provider shall:

1. Implement industry-standard encryption practices in its transmission of Personal Data. Industry-standard encryption methods used by Provider includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec).

2. If technically feasible, encrypt all Personal Data, including, in particular, any sensitive Personal Data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by Provider. The Provider's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document.

3. For Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including RSA's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation, and other common attack methods.

INFRASTRUCTURE SECURITY & CONNECTIVITY. If: (a) the Solutions include application, website, data, or system hosting, (b) network connectivity is required to provide the Solutions, or (c) the Solutions are dependent on the integrity of Provider's environment, the following requirements shall apply:

1. The connection and mechanism to transmit RSA Data between Provider and RSA shall be through an RSA IT- approved secure solution. Duration of access shall be restricted to only when access is required. Provider shall use Appropriate Safeguards to protect against any compromise, unauthorized access, or other damage to RSA's network and to secure the Provider's networks and IT environments associated with the Solutions. Upon request, Provider shall provide RSA with a high-level network diagram that outlines Provider's IT network supporting the Solutions.
2. Upon request, Provider shall provide a controls audit report and remediation effort, such as a SSAE 16 or information security audit performed within the past year, as applicable to the Solutions. The audit shall include an assessment of Provider's applicable general controls and security processes and procedures to ensure compliance with Privacy Laws and industry standards. The audit shall be at Provider's expense as part of Provider's ongoing information security program to evaluate Provider's general security controls.
3. In addition to Provider's internal control programs, Provider will have independent penetration tests performed on its environment as relevant to this DPA not less than once year and will perform security vulnerability scans not less frequently than quarterly. Provider commits to remediate all vulnerabilities identified in a timeframe commensurate with the risk, or as agreed upon with RSA.

SYSTEM ACCESS CONTROLS. Access to Provider's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted to prevent access from unauthorized individuals. Such procedures include:

1. **Admission controls** (i.e., measures to prevent unauthorized persons from using data processing systems):
   (a) Access is provided based on segregation of duties and least privileges to reduce the risk of misuse, intention or otherwise.
   (b) Access to IT systems will be granted only when a user is registered under a valid username and password.
   (c) Provider has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen, or compromised.
   (d) Mandatory password changes on a regular basis.
   (e) Automatic computer lock, renewed access to the PC only after new registration with a valid username and password.
   (f) Data and user classification determines the type of authentication that must be used by each system.
   (g) Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.
2. **Access controls** (i.e., measures to prevent unauthorized access to systems):
   (a) Access authorization is issued in respect of the specific area of work the individual is assigned to (i.e., work role).
   (b) Adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason.
   (c) Granting, removing, and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question.
   (d) Event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

DATA ACCESS CONTROL. Provider applies the controls set out below regarding the access and use of Personal Data:

1. Personnel are instructed to only use the minimum amount of Personal Data necessary to achieve the Provider's relevant business purposes.

2. Personnel are instructed not to read, copy, modify, or remove Personal Data unless necessary to carry out their work duties.
3. Third party use of Personal Data is governed through contractual terms and conditions between the third party and Provider which impose limits on the third party's use of Personal Data and restricts such use to what is necessary for the third party to provide services.

SEPARATION CONTROL. Where legally required, Provider will ensure that Personal Data collected for different purposes can be Processed separately. Provider shall also ensure there is separation between test and production systems.

AVAILABILITY CONTROL. Provider protects Personal Data against accidental destruction or loss by following these controls:

1. Personal Data is retained in accordance with the Provider Agreement or, in its absence, Provider's record management policy and practices, as well as legal retention requirements.
2. Hardcopy Personal Data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable.
3. Electronic Personal Data is given to Provider's IT Asset Management team for proper disposal.
4. Appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

DATA INPUT CONTROL. Provider has, where appropriate, measures designed to check whether and by whom Personal Data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded. Provider shall ensure that: (a) all account actions can be traced to the individual using the account, (b) the time, date and type of action is recorded for all privileged account actions and all account actions affecting RSA Data, (c) all recorded account actions are actively monitored and can be easily retrieved for analysis, and (d) consequences for policy violations are established, communicated, and acted upon.

SYSTEM DEVELOPMENT AND MAINTENANCE. Publicly released third party vulnerabilities are reviewed for applicability in the Provider environment. Based on risk to Provider's business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance. Provider shall ensure that policies are related to: (a) structured vulnerability management, including regular scanning, penetration testing, risk analysis and timely patching, (b) change management, including documentation of the purpose, security impact analysis, testing plan and results, and authorization for all changes, (c) configuration management, including secure baseline configurations, and (d) monitoring to detect and generate alerts for unauthorized changes.

COMPLIANCE. The IS, legal, privacy, and compliance departments work to identify regional laws and regulations that may be applicable to Provider. These requirements cover areas such as intellectual property of the Provider and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements. Mechanisms such as the information security program, the privacy reviews, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews, and risk management combine to drive compliance with these requirements.

Annex III

Annex III to the EU Standard Contractual Clauses. List of Sub-Processors.

[Answer]

Annex IV

UK Standard Contractual Clauses

The following designations and amendments apply to the UK Standard Contractual Clauses:

1. Part 1, Table 1: the Parties to the UK Standard Contractual Clauses shall be in accordance with “Annex I to the EU Standard Contractual Clauses”.
2. Part 1, Table 2: the relevant designations are in accordance with Section 9.2 of the DPA, unless such designations contradict or conflict with the UK Standard Contractual Clauses, in which case the UK Standard Contractual Clauses shall apply.
3. Part 1, Table 3:
    a. Annex 1A and Annex 1B are in accordance with “Annex I to the EU Standard Contractual Clauses”.
    b. Annex II is in accordance with “Annex II to the EU Standard Contractual Clauses. Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data”.
    c. Annex III is in accordance with “Annex III to the EU Standard Contractual Clauses. List of Sub-Processors.”
4. Part 1, Table 4: the following selections apply: "Importer” and “Exporter”.