**ADAPTIVE AUTHENTICATION LICENSE SCHEDULE**
for deployment in a
**CLOUD ENVIRONMENT**

***** IMPORTANT INFORMATION – PLEASE READ CAREFULLY *****

**This RSA Adaptive Authentication software uses computer programs and other proprietary material and information, the use of which is subject to and expressly conditioned upon acceptance of this Adaptive Authentication License Schedule (the "License Schedule").**

**This License Schedule is subject to the: (i) the End User License Agreement for RSA Products; (ii) Maintenance Agreement for RSA Products; and (iii) the RSA Cloud Services Schedule ("Cloud Schedule"), all located at http://www.emc.com/support/rsa-standard-form-agreements.htm and the terms of which are incorporated herein by reference (collectively referred to as the "Agreement").**

**This License Schedule is a legally binding document between you (meaning the individual person or the entity that the individual represents that is subscribing to the Software for its internal productive use and not for outright resale) (the "Customer") and RSA (which means (i) RSA Security LLC, if Customer is located in the United States, Mexico or South America; (ii) the local EMC Corporation sales subsidiary, if Customer is located outside the United States, Mexico or South America and in a country in which EMC Corporation has a local sales subsidiary; and (iii) EMC Information Systems International ("EISI"), if Customer is located outside United States, Mexico or South America and in a country in which EMC Corporation does not have a local sales subsidiary). Unless RSA agrees otherwise in writing, this License Schedule governs Customer's use of the Software, except to the extent all or any portion of the Software is: (a) the subject of a separate written agreement set forth in a quotation issued by RSA; or (b) governed by a third party licensor's terms and conditions. Capitalized terms have meaning stated in the License Schedule.**

**By clicking on the "Agree" or "Accept" or similar button at the end of this License Schedule, or proceeding with the installation, downloading, use or reproduction of the Software, or authorizing any other person to do so, you are representing to RSA that you are (i) authorized to bind the Customer; and (ii) agreeing on behalf of the Customer that the terms of this License Schedule shall govern the relationship of the parties with regard to the subject matter in this License Schedule and are waiving any rights, to the maximum extent permitted by applicable law, to any claim anywhere in the world concerning the enforceability or validity of this License Schedule.**

**If you do not have authority to agree to the terms of this License Schedule on behalf of the Customer, or do not accept the terms of this License Schedule on behalf of the Customer, click on the "Cancel" or "Decline" or other similar button at the end of this License Schedule and/or immediately cease any further attempt to install, download or use this Software for any purpose, and remove any partial or full copies made from this Software.**

**1.** **Definitions.** The defined terms in this License Schedule shall have the definitions set forth immediately below or set forth elsewhere herein. Capitalized words used in this License Schedule and not expressly defined herein will have the meaning stated in the Agreement.

"**Data Services**" means:

i. updates to the RSA eFraudNetwork made available to Customer by RSA via the RSA servers.
ii. data and information derived from the Geo-Location Service (as used herein, "Geo-Location Service" means the geo-location component available with the Software).

"**Documentation**" means the then-current, generally available, written user manuals and online help and guides provided by RSA for the Software.

"**RSA eFraudNetwork**" means a service owned and operated by RSA which contains information aggregated by RSA, discovered by the parties as part of the performance of their obligations under this License Schedule, obtained, and/or procured from third parties and/or resulting from risk and fraud assessments carried out by RSA and includes without limitation IP addresses, cookies and any other related data. The RSA eFraud Network will not include any information which would allow the holder thereof to identify an End User.

"**End User**" means a client of Customer, whose transaction may be processed by the Software pursuant to this License Schedule.

"**Maintenance Services**" shall mean the support service provided by RSA as set out the Maintenance Agreement for RSA Products and in section 6 below.

"**Software**" shall mean the selected components of RSA's Adaptive Authentication software as set out in section 3 below.

"**Transaction**" means all Software functional activities as set out in section 3 except for, Case Management API and Additional Features. For purposes of clarity, a Transaction includes all requests sent by Customer to RSA.

**2.** **Purpose.** This License Schedule enables the Customer to use the Software in Microsoft's Windows Azure IaaS (infrastructure as a Service) environment, an Internet-scale cloud computing and services platform hosted in Microsoft data centers(the "**Cloud Environment**"), This License Schedule governs the scope of the Software's license in relation to the Cloud Schedule. Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between the terms of the Agreement and this License Schedule, the terms of this License Schedule shall prevail solely with respect to the subject matter hereof. The Software licensed hereunder will be implemented by RSA as a multi-tenanted installation in an environment which employs shared infrastructure while segregating customer data ("**Deployed Software**").

**3.** **Software Features.** The Software provides the following functionality:

| **Risk Based Authentication of Transactions** |
|---|
| Assessment, analysis and scoring of login and post-login activities (in the online and mobile channels) by a Bayesian, self-learning risk engine that leverages both device and behavioral profiling. A case management application allows investigating high risk transactions, marking the fraudulent ones, and feeding feedback into the risk engine. A partial list of such post-login transaction activities includes but is not limited to: transferring funds, making online payments, establishing payees, personal information, etc. |
| **Case Management API** |
| The Case Management API allows organizations to programmatically integrate RSA Adaptive Authentication case management application with other third-party or in-house fraud detection systems, repositories, reporting and case management systems, and investigation tools that they are already using.<br>• The Case Management API allows organizations to: extract cases and activities from the case management application to their organization systems using an API<br>• Investigate the cases in their custom application; and<br>• Update the case statuses in Adaptive Authentication case management application |
| **Optional Additional Features – Authentication Methods**<br>**NOTE:** Additional fees will apply if these features are selected.<br>If selected, the fees will be set forth in the RSA Quotation |
| *Out of band phone call.* Out-of-band phone call (telephone confirmation using telephone numbers stored in Customer's systems)feature involves set up costs and fees to make the phone calls (one time third party set up fee; onetime RSA setup fee; fee per phone call).<br>*Out-of-band SMS*. One Time Password generated by Adaptive Authentication and sent by RSA to end user via SMS. The out-of-band SMS feature involves set up costs and fees to send the SMS (one time third party set up; onetime RSA set up fee; and a per SMS message fee). Out of band ("**OOB**") phone call / SMS is provided via third parties and infrastructure not owned/controlled by RSA. Delivery of calls/messages (or the timing of delivery) is not guaranteed. RSA's warranties and/or indemnities do not extend to nor apply to OOB services. |

**4.** **Term & Termination.** The initial term of this License Schedule shall commence on the date the applicable RSA Quotation is accepted by the Customer and shall end on the third anniversary of the Software's implementation in accordance with the terms of the Implementation SOW (the "**Initial Term**"). This License Schedule shall automatically renew for additional one (1) year terms (each a "**Renewal Term**") unless either party sends the other written notice of termination at least sixty (60) days prior to the end of the Initial Term or the applicable Renewal Term in which case this License Schedule shall terminate at the end of the Initial Term or such Renewal Term. The Initial Term and the Renewal Term are referred to together as the "**Term**".

**5.** **Software Authorized Use.** For so long as this License Schedule remains in force and subject to the terms and conditions of the Agreement, RSA hereby grants Customer a non-exclusive, non-transferable right to access and use the Deployed Software for assessing the risk of Transactions, in accordance with the instructions contained in the Documentation and subject always to the scope and pricing specified in the applicable RSA Quotation. Customer will not directly or indirectly use Software for its internal enterprise authentication purposes. As used herein, "internal enterprise authentication" means authenticating a request (which request may originate either remotely or from Customer or an Affiliate's premises) of an employee, consultant, or an agent of Customer (or an Affiliate) for the purpose of granting the requestor access to Customer (or an Affiliate's) computer networks for the purpose of performing their assigned job/work. All rights not expressly granted herein with respect to the Software are reserved to RSA. Nothing contained herein shall limit RSA's right to license or otherwise distribute or make available to any third party, develop, use, create derivative works of, or otherwise exploit the RSA Software (and the underlying RSA products and services), in whole or in part.

6. **Cloud Environment**. The Deployed Software shall be implemented in the Cloud Environment. The Software is designed to utilize the data security features of Microsoft's Azure platform to protect Customers data. The terms set forth in the Cloud Schedule shall apply to the Deployed Software that is implemented in the Cloud Environment. The Cloud Schedule shall supersede and control over any conflicting terms and conditions, order document, acknowledgment or confirmation, or other document issued by Customer, unless RSA executes a written agreement with Customer expressly indicating that the other document will modify the Cloud Schedule.

7. **Software Implementation.** The implementation plan for the Customer will be set out in a separate statement of work (the "**Implementation SOW**"). The Implementation SOW will detail the final delivery project scope and the Customer specific configuration and implementation of the Deployed Software. The parties will cooperate as reasonably necessary and in a timely manner to complete the implementation process described in the Implementation SOW.

8. **Maintenance Services:** Enhanced Support and Data Services are bundled with the Software for the duration of the Term. Customer will not (a) reproduce or distribute the Geo-Location Service in a manner that allows its users to access the Geo-Location Service in any way other than through aggregate reports generated by the Software (as described in the Documentation); or (b) use the data and information derived from the Geo-Location Service to create or otherwise support the transmission of unsolicited commercial email.

9. **RSA eFraudNetwork Data.** RSA shall retain and own all right, title and interest and all intellectual property rights (including but not limited to copyrights, trade secrets, trademarks and patent rights) to all information which is collected, submitted to and made available on the RSA eFraudNetwork database in the course of the performance by either party of their obligations under the Agreement or this License Schedule (or where such title cannot be granted or otherwise transferred to RSA then Customer agrees to grant RSA an unconditional, unlimited, unrestricted, royalty free license to use, distribute and/or otherwise make available such information). Customer will: (i) not use any robot, spider, site search or other retrieval application or device to scrape, retrieve or index nor attempt to (a) identify any individual or any device and/or (b) extract any personally identifying information from data in the eFraud Network; (ii) not send any End User's data to RSA if such end user withholds or withdraws their consent to the collection of data by the Customer; and (iii) only use data provided by RSA strictly in conjunction with the use of the Software.

10. **Software Data Integrity.** The Deployed Software as implemented within the Cloud Environment, is designed to process Customer data in the following manner:
    i. within a virtual network ("Vnet").
    ii. connectivity between the Vnets across different regions routes are over a secure Vnet-to-Vnet (VPN) tunnel.
    iii. in a 3-tier design, namely a web, app and data tier. Each tier is deployed in a separate subnet and each subnet is protected by RSA defined and managed ACL's for in/out-bound traffic. RSA uses a messaging middleware between the web and app tier to prevent a direct access from web tier to app tier.
    iv. leverage proxy servers for the in/out-bound internet traffic routed to/from the production level Vnet.
    v. segregate between management and production Vnets.
    vi. not allow remote access direct to production systems.
    vii. all sensitive data and configuration parameters are encrypted on a per customer basis. All virtual machine images are hardened in accordance with industry standards.
    viii. data encryption keys are maintained on a per customer basis (the data encryption keys are rotated automatically on a weekly basis).
    ix. all application and system log files (including an audit trail of access to the back office functions, for example the customer facing applications – Case Management, Policy Management, etc) are retained in accordance with RSA's data retention policies.
    x. the data source for access management by RSA enforces the use of strict password policy for RSA administrators and Customer administrators.
    xi. RSA performs authorized access to all data sources and uses IP restriction rules for the management of the incoming traffic. All Customer communications in/out-bound are managed through SSL certificates issued for a Customer specific FQDN.
    xii. If the Deployed Software is:
        a. a new implementation, the following shall apply: If any Customer sensitive data (for example, account numbers) is to be submitted to RSA, such data shall be hashed with SHA256 by the Customer before submission to RSA. RSA is not responsible for protecting any unhashed sensitive data that may be sent to and received by RSA.
        b. an implementation that was upgraded from version 11 of the Software, the following shall apply: If any Customer account numbers are to be submitted to RSA, such account numbers will continue to be hashed by RSA upon receipt by RSA for a period of twelve (12) months counted from the date of the Customer's switch over to version 12 of the Software. Upon expiry of such period, paragraph xii.a. above shall apply.
    xiii. Upon at least ninety (90) days prior written notice to RSA and no more frequently than once every twelve (12) months during the Term, RSA will permit Customer to review selected samples of RSA's security policies directly related to the Deployed Software during an onsite visit to RSA's Executive Briefing Center ("EBC") during RSA standard business hours. Customer will not be given physical access to data operations centers,

the Cloud Environment and other like premises that are subject to restricted access. The Customer is responsible for any costs and expenses which Customer incurs in connection with the onsite visit to the EBC.

ivx. RSA shall maintain effective internal controls consistent with industry standards to monitor compliance with this section 10. RSA shall maintain complete and accurate records in English. During the Term and for a period of three (3) years thereafter, or longer if required under applicable law, upon receipt of 45 days advanced written notice, RSA shall provide to Customer, its agents, auditors and government regulators a 'certificate of compliance' duly signed by RSA's chief information security officer in order to verify compliance with this section.

**11. Scoring & Response Time Benchmarks.**

i. Transaction scoring: 95% of the transactions will be scored within no more than one second, and 99.5% of transactions shall be scored within no more than four seconds. Note: transaction scoring term shall be measured from the moment RSA received the request till submission of score.

ii. Out-of-band phone call: Telephone calls shall be initiated (i.e., allocate a telephone line for the call and go off-hook and begin to dial) approximately within ten (10) seconds from receiving the request from Customer 95% of the time and in no event within more than sixty (60) seconds of receiving the request from Customer.

iii. Out-of-band SMS: Generally 90% of SMS messages bound to the applicable carrier will processed by the SMS aggregator within five (5) seconds and 99% of the SMS messages bound to the applicable carrier will processed by the SMS aggregator within fifteen (15) seconds.

Customer acknowledges that the scoring and/or timeliness of the above benchmarks are not guaranteed by RSA. RSA does not assume and shall not be responsible for performance delays or failures (including without limitation latency, scheduled downtime, etc.) attributed to any non-RSA platform and/or network. Upon Customer request, RSA will provide a transaction scoring report to Customer no later than the 14th day of the month following the reporting period,

**12. Payment.** Customer shall pay RSA the applicable fees as outlined in the RSA Quotation.

**13. Consents.** Any type of data collected by the Customer from its End Users (including without limitation such users' device, location) and any form of processing, maintenance, uploading, syncing, or transmission thereof must comply with all applicable privacy and data collection laws and regulations. Customer is solely responsible for:

i. informing its users about the specific types of data that Customer will collect and the purpose thereof;

ii. obtaining the users' documented consent to such collection;

iii. displaying a conspicuous visual indicator when such data is being collected; and

iv. not disable, override or otherwise interfere with any RSA implemented system alerts, warnings, display panels, consent panels and the like intended to notify the end user.

**14. Privacy Legislation.** Except as required for the proper performance of the party's obligations under this License Schedule, the parties do not intend to disclose to one another hereunder information that would be covered by the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of 1996 or similar privacy legislation within or outside of the United States. Accordingly, neither party shall disclose to the other hereunder any of the following information regarding either party's employees, customers, suppliers or other business partners: protected health information (as defined at 45 CFR 164.501), social security numbers, driver's license numbers, credit card numbers or similar government identity numbers or personal account numbers. RSA shall not be liable for any claim by Customer's customers', including End Users' or other third parties arising from the unauthorized or fraudulent application for, access to or use of such personal data and Customer shall indemnify RSA for all third party claims arising as a result of Customer's breach of this obligation.

**15. RSA Trademark License**. For so long as this License Schedule remains in force RSA grants Customer the right to use the "Secured by RSA" trademarks described herein below (the "**RSA Mark**") solely for the purpose of displaying the RSA Mark on the End User facing web based log in pages of its online services. Customer's use of the RSA Mark will conform at all times with RSA's quality and usage requirements and will be subject to prior review and approval by RSA. Customer will not seek to register any trademarks of RSA in any country in the world. Any use of the RSA Mark shall be in accordance with RSA's reasonable policies regarding advertising and trademark usage as established from time to time. Nothing else herein shall prevent Licensee from separately branding its security processes which may use the Licensed Software and other security processes.

**16. Reference.** RSA may identify Customer for reference purposes.