Agreement for Digital Signing Service

This Agreement for Digital Signing Service (the "Agreement"), together with the attached schedules, is made between GMO GlobalSign, Inc., of Two International Drive, Suite 150, Portsmouth, NH 03801 ("GlobalSign") and _____ of _____ ("Customer") as of _____ (the "Effective Date") and governs Customer's use of the GlobalSign digital signing service, a hosted service under which Customer submits requests for short-lived digital signing Certificates and uses them to sign a hash of a document, and GlobalSign generates such Certificates and provides related services to Customer on an outsource basis as further described in Schedule A (the "Service").

1. Definitions

For the purposes of this Agreement, all capitalized terms used in this Agreement shall have the meaning ascribed to them in this Section 1 and elsewhere in this Agreement.

AATL Technical Requirements: The then current version of the Adobe Approved Trust List Technical Requirements available at https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html#AATLtechnicalrequirements.

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0 and later.

API Authentication Account: A unique account for Customer that identifies Customer identity and enables Customer to connect to the Service.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certification Authority (CA): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. GlobalSign is the CA hereunder.

CPS: GlobalSign's Certification Practice Statement available at http://www.globalsign.com/repository/.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Electronic Seal: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

Governmentally Accepted Form of ID: A physical or electronic form of identification (ID) issued by the local country/state government, or an ID issued or generated by a third party that the local government accepts for validating identities of Individuals for its own official purposes.

ID Source: Any of (i) A Governmentally Accepted Form of ID; (ii) copy of an attestation from an appropriate notary or Trusted Third Party that s/he has verified the Individual identity based on a Governmentally Accepted Form of ID, or (iii) copy of a video recording of the verification of Individual identity using secure video communication.

Identity Verification Process: The method used by Customer to verify the identity of an Individual, including the setup, ID Sources, security procedures, and other implementation details. The Identity Verification Process must comply with the AATL Technical Requirements and must be pre-approved by GlobalSign.

Individual: A natural person.

Individual External Identities: The identity of an Individual associated with a partner or a consumer, or other relationship with Customer for purpose of conducting business with Customer.

Individual Internal Identities: The identity of an Individual who is an employee or contractor associated with the Customer's Organization Validated (OV) Certificate Profile(s).

Key Pair: The Private Key and its associated Public Key.

Local Registration Authority (LRA): The appointed entity (other than GlobalSign) that is responsible for verifying the identity and information stipulated in the Certificate for Subscribers who are affiliated with Customer's Organization Validated (OV) Certificate Profile, in order to submit requests on their behalf to the Service. The Customer shall be the LRA and will be restricted to approving and requesting Certificates using its Organization Validated Certificate Profile.

Organization Validated (OV) Certificate Profile**:** A pre-approved Certificate template that restricts Certificate request and issuance to a specific organization that has been verified by GlobalSign using GlobalSign's OV vetting process.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Relying Party: Any natural person or legal entity that relies on a valid Certificate.

Subscriber: A natural person or legal entity to whom a Certificate and digital signature is issued and who is legally bound by a Subscriber Agreement.

Subscriber Agreement: An agreement between the CA and the Subscriber that specifies the rights and responsibilities of the parties.

Trusted Third Party: A third party approved by GlobalSign that maintains a secure process used by Customer for its Identity Verification Process as may be permitted by the AATL Technical Requirements.

2. Use of the Service. GlobalSign hereby grants to Customer the right to use the Service under the terms set forth in this Agreement. Customer shall use the Service only for purposes that are permitted by this Agreement, and any applicable laws and regulations, including without limitation, any laws regarding the use and transfer of personal data.

3. Limitations on Use. Customer shall not (a) use the Certificates or API except as permitted by this Agreement, (b) distribute or resell the Service to any third party unless explicitly permitted in this Agreement, (c) cause or permit the reverse engineering, disassembly, or decompilation of the Digital Signatures or the Certificates, or (d) exceed the number of signings permitted under the license pack purchased by Customer.

4. Fees; Payment. Customer agrees to pay GlobalSign for the Service in accordance with the fees stated in Schedule B. All payments are due and payable in U.S. dollars net thirty (30) days from the invoice date. Interest shall accrue at the rate of one and one-half percent (1.5%) per month on all overdue amounts. Customer will pay any taxes, fees and similar governmental charges related to the execution or performance of this Agreement, other than applicable income taxes imposed on GlobalSign related to its receipt of payments from Customer.

5. Term; Termination. The initial term of this Agreement will begin on the Effective Date and, unless terminated earlier in accordance herewith, will continue for a period of one (1) year ("Initial Term"). This Agreement will renew automatically on the same terms and conditions for additional successive periods of one (1) year (each, a "Renewal Term") unless either party gives the other written notice of its intention not to renew at least thirty (30) days prior to the end of the then current term.

This Agreement may be terminated immediately by either party upon written notice if (a) the other party breaches any of the terms of this Agreement and such breach continues for a period of thirty (30) days after notice thereof has been given by a party; (b) the other party files for bankruptcy, ceases to carry on business, or undergoes liquidation; or (c) the other party is unable to perform a material portion of its obligations under this Agreement as a result of an event or events of *force majeure* for a period of not less than thirty (30) days. Notwithstanding 5(a) above, this Agreement may be terminated immediately by GlobalSign upon written notice if GlobalSign determines, in its reasonable discretion, that Customer poses a security risk to the Service or other GlobalSign system.

6. Effect of Termination. Upon termination of this Agreement in any manner, (1) Customer shall immediately pay GlobalSign any outstanding fees; (2) Customer shall have no right to use the Service, and the terms and conditions of this Agreement shall continue to apply to any Digital Signatures created prior to the termination until the expiration or earlier revocation of the Certificate; and (3) all rights and obligations of the parties under this Agreement shall cease immediately except the following Sections which shall survive any expiration of termination: 3, 5, 9, 10, 11, and 13 - 16.

7. Warranty and Disclaimer

7.1 GlobalSign Warranties. GlobalSign warrants that:

(a) Compliance with Laws. GlobalSign shall comply with all applicable federal, state, and local laws and regulations applicable to GlobalSign's provision of the Service. GlobalSign shall have all professional licenses, permits, certificates and registrations required for its performance of the Service.

(b) Authority. GlobalSign is validly existing and in good standing under the laws of the jurisdiction of its organization and has the power and authority to enter into this Agreement. This Agreement has

been duly executed and delivered by GlobalSign and constitutes the valid and binding obligation of GlobalSign.

(c) No Other Warranty. Except as provided in the GlobalSign Certification Practice Statement at https://www.globalsign.com/repository/, the Service and Certificates are provided on an "as-is", "as available" basis, and GlobalSign does not make any and hereby specifically disclaims any representations, endorsements, guarantees, or warranties, express or implied, to Customer, Certificate users, or any other person, including, without limitation, any: (i) of merchantability, fitness for a particular purpose, title, or noninfringement of intellectual property rights; (ii) arising from course of dealing, course of usage, course of performance, or course of trade or trade practice; and (iii) of quality, timeliness, accuracy, reliability or content.

7.2 Customer Warranties. Customer warrants that:

(a) Compliance with Laws. Customer shall comply with all applicable federal, state, and local laws and regulations. Customer shall have all professional licenses, permits, certificates and registrations required for its use of the Services.

(b) Authority. Customer is validly existing and in good standing under the laws of the jurisdiction of its organization and has the power and authority to enter into this Agreement. This Agreement has been duly executed and delivered by Customer and constitutes the valid and binding obligation of Customer.

(c) Subscriber Information. Customer warrants that all information and representations made by the Subscriber are true.

(d) Personal Information. Customer warrants that (i) it has the necessary rights to provide any personal data or other information that Customer to GlobalSign, and (ii) providing such information does not violate any applicable data privacy law, contract or privacy policy.

8. Confidentiality

8.1 "Confidential Information" means all information that is provided or made available to one party (the "Receiving Party") by the other party (the "Disclosing Party"). Confidential Information includes, but is not limited to: inventions, technologies; strategies; trade secrets; customer and supplier lists; product designs and pricing information; processes; formulas; business plans; employer and consumer information; employee data; product licensing plans; budgets, finances, and financial plans; production plans and protocols; systems architecture, technology, data, and methods, and any other information that by its nature would typically be considered non-public information. Confidential Information may be conveyed to the Receiving Party in written, electronic, or oral form, and includes any information that may be derived from or developed as a result of access to the Disclosing Party's facilities, as well as all notes, reports, evaluative materials, analyses or studies prepared by the Receiving Party or its directors, officers, employees, agents and advisors (collectively, such Party's "Representatives") regarding or relating to the Disclosing Party or its Confidential Information.

8.2 The Receiving Party will protect, and will ensure its employees, officers, agents and contractors will protect Confidential Information by using the same degree of care as Receiving Party uses to protect its own Confidential Information of a like nature (but no less than a reasonable degree of care) to prevent the unauthorized use, dissemination, disclosure or publication of such Confidential Information. The Receiving Party may disclose the Confidential Information only to those of its affiliates and their respective employees and advisors who have a need to know and who are under an obligation of confidentiality at least as restrictive as that contained herein. GlobalSign

may also may disclose the Confidential Information as may be required for GlobalSign to fulfill its obligations under the Adobe AATL program, subject to appropriate confidentiality provisions. Confidential Information received may be used only to fulfill the purposes of the Agreement. If a Receiving Party or any of its respective affiliates is requested or required by subpoena, court order, or similar process or applicable governmental regulation to disclose any Confidential Information, Receiving Party agrees to provide the Disclosing Party with prompt notice of such request or obligation so that the Disclosing Party may seek an appropriate protective order or procedure if it elects to do so. The Receiving Party's obligations with respect to particular Confidential Information will expire three (3) years after the termination of this Agreement.

8.3 The foregoing confidentiality obligations will not apply to Confidential Information that (a) is now or subsequently becomes generally available to the public through no fault or breach on the part of the Receiving Party; (b) is known by the Receiving Party prior to disclosure as noted by tangible record; (c) is independently developed by the Receiving Party without the use of any Confidential Information of the Disclosing party; or (d) the Receiving Party rightfully obtains without a duty of confidentiality from a third party who has the right to transfer or disclose it; (e) is disclosed under operation of law; or (f) is disclosed by the Receiving Party with the prior written approval of the disclosing party.

9. Ownership. Except for the rights expressly granted under this Agreement, all right, title and interest in and to the Service is owned exclusively by GlobalSign. GlobalSign retains all right, title, and interest in and to the Service and all other products, works, and other intellectual property created, used, or provided by GlobalSign for the purposes of this Agreement, and all modifications, improvements and derivative works of the same.

10. Indemnification

10.1 GlobalSign will settle and/or defend at its own expense and indemnify and hold harmless Customer against any cost, loss or damage from any claim, demand, suit or action brought by a third party against Customer (i) arising out of or related to (i) GlobalSign's breach of any warranties contained in this Agreement, or (ii) alleging that use of the Service by Customer as permitted hereunder infringes upon any copyright, trademark, trade secret, U.S. patent or other intellectual property right of any third party.

Should the Service become, or in GlobalSign's sole opinion likely to become, the subject of any claim or action for infringement, GlobalSign may (a) procure for Customer the right to continue using the Service as contemplated hereunder at no cost to Customer; (b) modify the Service, without loss of material functionality or performance, to render the Service non-infringing; or (c) if the foregoing alternatives are not reasonably available to GlobalSign, terminate this Agreement.

GlobalSign's indemnification obligation will not apply to infringement actions or claims to the extent that those actions or claims are based on or result from: (i) modifications made to the Service by or on behalf of Customer, or (ii) the combination of the Service with items not supplied by GlobalSign.

10.2 Customer will settle and/or defend at its own expense and indemnify and hold harmless GlobalSign against any cost, loss or damage from any claim, demand, suit or action brought by a third party against GlobalSign arising out of or related to (i) Customer's breach of any warranties contained in this Agreement, and (ii) any use of or reliance on the Service, Digital Signature or a Certificate, including but not limited to claims related to Certificate issuance or revocation or private key compromise; provided, however, that Customer shall not be obligated to indemnify GlobalSign for any

loss, costs, damages or expenses caused by the intentional misconduct or gross negligence of GlobalSign.

10.3 The party seeking indemnification (the “Indemnified Party”) agrees to promptly notify the party providing indemnification (the “Indemnifying Party”) in writing of any indemnifiable claim. The Indemnifying Party shall control the defense and settlement of an indemnifiable claim. The Indemnified Party shall cooperate in all reasonable respects with Indemnifying Party and its attorneys in the investigation, trial, defense and settlement of such claim and any appeal arising therefrom. The Indemnified Party may participate in such investigation, trial, defense and settlement of such claim and any appeal arising therefrom, through its attorneys or otherwise, at its own cost and expense.

11. Limitation of Liability. GlobalSign’s aggregate liability to Customer (either directly or as a third party defendant in any action or proceeding) for any and all claims arising out of or relating to this Agreement, or the use of or inability to use the Service, Digital Signatures or Certificates will in no event exceed the amount of fees paid by Customer for the Service, Digital Signatures and/or Certificates within the one (1) year period immediately prior to the event that gave rise to its claim.

12. Limitation of Damages. GlobalSign shall not be liable to Customer for any special, consequential, incidental or indirect damages including, but not limited to, loss of profits, revenue, or damage to or loss of data arising out of the use of or inability to use the Service or Certificates whether or not GlobalSign has been advised of the possibility of such damages.

13. Force Majeure. Neither party shall be liable for failure or delay in performing its obligations hereunder if such failure or delay is due to circumstances beyond its reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike or other, interruption of or delay in transportation, unavailability of interruption or delay in telecommunications or third party services; provided however, that if a party suffering a force majeure event is unable to cure that event within thirty (30) days, the other party may terminate this Agreement.

14. Notices. Notices shall, unless otherwise specified herein, be in writing and may be delivered by hand delivery, United States mail, or overnight courier service. Notices shall be effective at the close of business on the day actually received, if received during business hours on a business day, and otherwise shall be effective at the close of business on the next business day. A party may change its contact information below by providing notice of same in accordance herewith.

Notices to Customer shall be sent to:

[*insert Customer notice address*]

Notices to GlobalSign shall be sent to:

GMO GlobalSign, Inc.
2 International Drive, Suite 150
Portsmouth, NH 03801
Attn: General Counsel

15. Miscellaneous

15.1 Governing Law and Jurisdiction. This Agreement shall be governed by, construed under and interpreted in accordance with the laws of New Hampshire, USA without regard to its conflict of law provisions. Venue shall be in the courts of New Hampshire.

15.2 Assignment. Except as otherwise provided herein, this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. This Agreement may not be transferred or assigned by Customer without GlobalSign's prior written consent. Any such purported transfer or assignment shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

15.3 Severability. If and to the extent that any court holds any provision of this Agreement to be unenforceable, such unenforceable provision shall be stricken and the remainder of this Agreement shall not be affected thereby. The parties shall in good faith attempt to replace any unenforceable provision of this Agreement with a provision that is enforceable and that comes as close as possible to expressing the intention of the original provision.

16. Entire Agreement. This Agreement, any schedules hereto, and any documents incorporated herein by reference constitute the entire agreement between the parties and supersedes any prior written or oral agreement or understanding with respect to the subject matter thereof. In the event of any inconsistent or incompatible provisions, the order of precedence shall be: this Agreement, the Subscriber Agreement, and the CPS. The terms and conditions of any past, present or future purchase order submitted by Customer which alter, modify or conflict with the terms and conditions of this Agreement are void.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of Effective Date set forth above.

GMO GlobalSign, Inc.		**Customer**	
By:	_____	By:	_____
Print Name:	_____	Print Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Schedule A
Description of Service

1. General Description of the Service

The Service is intended for use by companies that want to apply Digital Signatures to documents (most commonly using AATL certificates) or other digital transactions, but don't require GUI management components or advanced certificate life cycle management features. It provides a web based RESTful Application Programming Interface (API) for Customer to send a hash of the document through the DSS API using Customer's API Client credentials to Globalsign to apply a Digital Signature using secure server held Private Keys and associated short-lived Certificates stored in GlobalSign data centers. Certificates issued from the Service will be established based on an on-boarding survey completed by GlobalSign using data provided by Customer.

There are three main identity configuration options for the Service:

1. Digital Signatures – Customer Individual Internal Identities within Customer Organization Validated (OV) Profile
2. Digital Signatures – Customer Individual External Identities within Customer Organization Validated (OV) Profile
3. Electronic Seals – A department within Customer's Organization Validated (OV) Certificate Profile

The specific features of the API service are documented at https://d9xqspohc21bf.cloudfront.net/acton/attachment/2674/f-08ca/1/-/-/-/-/GlobalSign-Signing-Service-API.html as may be updated by GlobalSign from time to time.

The RESTFUL API is a transactional API, which enables the following workflows:

- Allows API client to place a request to initiate a signing session.
- Allows API client to create a Certificate and digitally sign a hash.
- Allows API client to retrieve digitally signed hash for embedment into a .pdf document.

Certificate Revocation Services
GlobalSign will only provide an OCSP response when returned with the Certificate.

Customer Account Setup
In order to set up Customer's account, GlobalSign will perform the vetting for Customer's Organization Validated (OV) Certificate Profile.

- GlobalSign will set up and maintain a Customer API Authentication Account to enable Customer to use the Service.
- The Service will provide Customer with the ability to request Digital Signatures for the identity configuration option purchased by Customer, subject to Customer's vetted and approved 1) Organization Validated (OV) Certificate Profile and 2) Identity Verification Process.

Customer will designate one Individual (the "Administrator") with authority to (i) submit Customer organization identity information for verification by GlobalSign to create the Organization Validated Certificate Profile and (ii) approve the issuance of Certificates and Digital Signatures associated with Customer's Organization Validated Certificate Profile. GlobalSign will provide the Administrator with

API credentials for the purpose of issuing Digital Signatures. Customer's Administrator is identified in Schedule C.

The Administrator will be responsible for verifying the information in all Certificate and Digital Signature requests submitted to GlobalSign. GlobalSign shall not be responsible for verifying the accuracy or legitimacy of these orders.

If Customer wishes to change the designated Administrator or contact information provided in Schedule C**,** Customer must submit a new Designated Administrator form.

If Customer has opted to use a certificate hierarchy chained to one of GlobalSign's public root CAs, the Certificates and Service shall be provided in accordance with the then current GlobalSign Certification Practice Statement ("CPS") at https//www.globalsign.com/repository.

Prior to use of a Certificate, Customer shall ensure that any Individual requesting a Certificate agrees to the GlobalSign terms for use for the Certificate (the "Subscriber Agreement").

For purposes of this Agreement, the CPS, and Subscriber Agreement, the term "Subscriber" shall apply to Customer and not any employee of Customer in his/her capacity as an Individual. Customer, and not any such Individual, shall be legally responsible for compliance with any terms that are applicable to "Subscriber".

Customer shall:

- Ensure the APIAuth information is secure and accessible only by authorized persons.
- Ensure that information provided on the enrollment requests is complete and accurate.
- Promptly request that GlobalSign revoke the API Authentication Account access upon any actual or suspected loss, disclosure, or other compromise of the API Authentication Account information.
- If applicable, develop code and securely integrate into GlobalSign's API or software developer kit (SDK). For the avoidance of doubt, it is the sole responsibility of Customer to develop or integrate GlobalSign returned via API digitally signed hash and timestamp into their document management system.
- Provide written evidence as may be requested by GlobalSign from time to time in order to support demonstration of conformity with the AATL Technical Requirements.
- Confirm with the Subscriber that the information is correct before approving a Certificate request.
- Request revocation when any information related to the Certificate request has changed.
- Enter into and ensure compliance by each Individual Subscriber with the terms of the Subscriber Agreement, either directly or through the Service or through Customer's own workflow process. If Customer is issuing publicly trusted Certificates, the Subscriber Agreement must contain terms no less stringent than those in the GlobalSign subscriber agreement at https://www.globalsign.com/repository/.

2. Additional Obligations Based on Service Customer's Configuration Option

2.1 Individual Internal Identities

If Customer wishes to request Digital Signatures with Individual Internal Identities, Customer must:

- Act as the Local Registration Authority.
- Ensure that the Individual identity information submitted by Customer to request Certificate and Digital Signatures is an accurate representation of a current employee or contractor of Customer who has consented to the request.
- Create and keep detailed records of the Identity Verification Process.

2.2 Individual External Identities

If Customer wishes to request Digital Signatures with Individual External Identities, Customer must:

- Only issue Digital Signatures and Certificates to Individuals following GlobalSign's prior written approval of the Identity Verification Process against Customer's Organization Validated Certificate Profile.
- Promptly notify GlobalSign of any proposed changes to the Identity Verification Process. Customer may only implement any proposed changes after receipt of written approval from GlobalSign.
- Keep accurate written records of Identity Verification Process.
- Follow appropriate security procedures to ensure that the data used to generate the Certificate is true and valid to the ID Sources
- Notify GlobalSign in writing of any failure of Customer to comply with the identity verification obligations whether such failure becomes known to the Customer through its own internal audit or by other means.
- Certify in writing its compliance with the Identity Verification Process via a written attestation upon initial set up of the Service, annually and at any time within fourteen (14) days of request by GlobalSign.
- During the term of this Agreement and for one (1) year following termination, GlobalSign shall have the right to perform audits of Customer or a Trusted Third Party used by Customer (if applicable) to verify the Identity Verification Process, including the related processes and results of the Identity Verification Process. The number of records to be audited may vary from time to time as determined by GlobalSign in its reasonable discretion.
    - Customer will permit GlobalSign and/or its agents upon reasonable notice access to Customer books and records during normal business hours for the purpose of verifying Customer's performance of its obligations under this Schedule A. Such audit will be at the expense of GlobalSign and will not be performed more than once in each calendar quarter.
    - Within five (5) business days of GlobalSign's request, make available to GlobalSign (i) copies of the ID Sources used to perform the Identity Verification Process for the requested sample of issued Certificates, as may be requested by GlobalSign from time to time, and (ii) the name of the authorized representative of the Customer who will be responsible for acknowledging the audit observations.
    - Upon completion of any audit, Customer's authorized representative will sign the acknowledgement of the audit observations provided by GlobalSign within one (1) business day after GlobalSign has provided him/her with a copy of the audit observations.
    - The Customer may provide redacted or excerpted content as necessary to comply with any applicable data privacy law.
    - In the case of non-conformities, Customer must provide GlobalSign with evidences of implementation of mitigation measures and alternative controls for evaluation and approval by GlobalSign.

- Retain copies of the ID Sources used to perform the Identity Verification Process for seven (7) years.

As Certificates for digital signing must comply with various industry standards and AATL Requirements, GlobalSign reserves the right to request changes to or revoke its approval of a Local Registration Authority or an Identity Verification Process at any time. In the event of such a change, Customer must promptly comply with the request from GlobalSign to (a) implement requested changes; and/or (b) immediately stop issuance of Certificates and Digital Signatures for Individuals if requested by GlobalSign.

If a Certificate was not issued in compliance these obligations, GlobalSign may immediately revoke the applicable Certificate.

The rights and remedies of GlobalSign set forth above are not exclusive of, but are cumulative to, any rights or remedies now or subsequently existing at law, in equity, by statute or otherwise.

2.3. Electronic Seals (not to be used for Individual based signings)

If Customer wishes to apply Electronic Seals to .pdf documents, Customer must:

- Only submit requests in the name of Customer's organization or an actual department in Customer's organization;
- Not submit requests in the name of an Individual; or
- Not submit requests that are inaccurate or misleading.

Schedule B
Fees and Payment Information

Customer agrees to pay GlobalSign the fees below for the Service. Customer may only request the type and quantity of signings purchased below. GlobalSign will not process requests that exceed the type or quantity of signings purchased by Customer except as noted below.

Fees for First Year

Item	Number of Permitted Signings[2]	Individual Internal Identities, Individual External Identities, or Electronic Seals	Maximum Throughput	Fee	Invoice Date
AATL signing license pack[1]			---- Signatures / Minute	$--------	Effective Date

First Year Total Amount Due: $

[1] Signing license packs expire 12 months from purchase. There is no credit or refund for expired unused signings.

[2] For Customer's convenience, GlobalSign will set up Customer's account to allow Customer to exceed the Number of Permitted Signings by ten percent (10%). If Customer exceeds the Number of Permitted Signings, GlobalSign will invoice Customer for the excess signings up to the ten percent (10%) maximum. The fee for each excess signing shall be on a per signature basis prorated based on the cost of the signing license pack purchased.

Customer Billing Contact Information

Name:
Address:

Phone:
Fax:
Email:

Schedule C
Designated Administrator

Name	Position	Cell Phone	Work Phone	Email