Verizon Northwest Inc.

P.O. Box 1003
Everett, WA 98206-1003
Fax: 425-261-5262

December 7, 2009

Washington Utilities and
Transportation Commission
P.O. Box 47250
1300 S. Evergreen Park Drive SW
Olympia, Washington 98504-7250



Subject: AFFILIATED INTEREST AGREEMENT – ADVICE NO. 415
Ref UT-051247

To whom it may concern:

Enclosed for the Commission's file is a verified copy of Amendment 54 to a Telecommunications Services Agreement between Verizon Services Organization Inc., on behalf of Verizon companies including Verizon Northwest Inc., and MCI Communications Services, Inc. The amendment adds Corporate SSL services. The footer notwithstanding, the companies are not seeking confidential treatment of this document.

Please call me at 425-261-5006 if you have any questions.

Very truly yours,

Richard E. Potter
Director
Public Affairs, Policy & Communications

Enclosure

VERIFICATION OF AFFILIATED INTEREST AGREEMENT

I verify that the enclosed is a true copy of Amendment 54 to a Telecommunications Services Agreement between Verizon Services Organization Inc., on behalf of Verizon companies including Verizon Northwest Inc., and MCI Communications Services, Inc.

Richard E Potter Date: 12-7-09

Richard E. Potter
Director
Verizon Northwest Inc.

AMENDMENT 54
TO THE
TELECOMMUNICATIONS SERVICES AGREEMENT
BETWEEN
VERIZON SERVICES ORGANIZATION INC.
AND
MCI COMMUNICATIONS SERVICES, INC.

This Amendment 54 to the Telecommunications Services Agreement (Contract No. TSA010302-1) ("Agreement") by and between MCI Communications Services, Inc. d/b/a Verizon Business Services, a Delaware corporation, with offices at 6929 N. Lakewood Avenue, Tulsa, Oklahoma 74117 ("Provider"), and Verizon Services Organization Inc., a Delaware corporation, with offices at 6665 N. MacArthur Boulevard, Irving, Texas 75039 ("Customer") shall be effective on the date set forth below.

1. EFFECTIVE DATE

This Amendment 54 shall be effective upon full execution by both parties. Notwithstanding anything to the contrary contained in this Agreement, the term of this Agreement and the other terms and conditions hereof, are subject to applicable law and regulatory approval. Accordingly, although this Amendment is executed by both Parties, to the extent that any state statute, order, rule or regulation or any regulatory agency having competent jurisdiction over one or both parties to this Agreement, shall require that this Amendment or any subsequent amendment be filed with or approved by such regulatory agency before the amendment may be effective, the Amendment shall not be effective in such state until the first business day after such approval or filing shall have occurred.

2. REGULATORY APPROVAL

This Agreement is subject at all times to any statute, order, rule, or regulation or any state or regulatory agency having competent jurisdiction over one or both of the parties hereto or the services provide hereby. Provider and Customer agree to cooperate with each other and with any applicable regulatory agency so that any and all necessary approvals may be obtained. During the term of this Agreement, the parties agree to continue to cooperate with each other in any review of this Agreement including subsequent amendments by a regulatory agency so that the benefits of this Agreement or such amendment may be achieved. If any such agency accepts this Agreement or any amendment in part and rejects it in part, or makes a material modification to the Agreement or amendment as a condition of its approval, either party may terminate the Agreement or Amendment in its entirety without penalty or liability.

3. AGREEMENT MODIFICATION

3.1 ADD a new Section 57, CORPORATE SSL SERVICES, to Exhibit C as set forth in Attachment 1.

4. OTHER TERMS AND CONDITIONS

Except as specifically amended herein, the terms and conditions of the Agreement, including any other Amendments thereto, shall remain in full force and effect during the term of the Agreement.

IN WITNESS WHEREOF the parties have entered into this Amendment 54 as of the date set forth above.

| MCI COMMUNICATIONS SERVICES, INC. | VERIZON SERVICES ORGANIZATION INC. |
|---|---|
| Catherine Hapiard | Dan Yong |
| Signature | Signature |
| Catherine Hapiard | Dan Yong |
| Print Name | Print Name |
| mgr- contract mgmt. | Senior Consultant - Sourcing |
| Title | Title |
| 11/5/09 | 11/2/09 |
| Date | Date |

ATTACHMENT 1

(ADD NEW SECTIONS 57 TO EXHIBIT C AS SET FORTH BELOW)

## 57 CORPORATE SSL SERVICES

From time to time and subject to mutual written agreement, orders for the provisioning of CorporateSSL services may be executed between the parties and each such order shall be incorporated into and made part of this Section 57 (each, an "Order"). Customer acknowledges that CorporateSSL services are offered and provided by Cybertrust, Inc., Provider's Affiliate.

### 57.1 License

57.1.1 Subject to the terms and conditions of this Section 57, Provider grants Customer, and Customer accepts, a non-exclusive, non-assignable, non-transferable, and revocable license to perform, for Customer's internal and legitimate business purposes only, the responsibilities and functions of a digital certificate registration authority ("RA") under the root hierarchy of the public certification authority ("Public CA") indicated in the Order. Except to the extent otherwise agreed in writing, Customer may request and authorize the issuance, suspension and revocation of digital certificates ("Certificate") for Authorized Users only (as defined herein). For the purposes of this Section 57, and unless explicitly set forth otherwise in the Order, "Authorized User" means any computer server on which Customer content only is hosted by or on behalf of Customer within the context of Customer's ordinary course of business, provided that the root domain names for which the computer server runs (i) must belong to Customer and be validly registered in Customer's name; (ii) must be pre-proofed by Provider and identified in the Order (or a subsequent executed change order).

57.1.2 Without prejudice to any further restrictions or limitations set forth in this Section 57, Customer may operate as RA for non-commercial purposes only, meaning that Customer may not and may not permit any third party to distribute any Certificate for the purposes of generating income.

57.1.3 Customer acknowledges that the CorporateSSL services provided hereunder by or on behalf of Provider are governed by the Public CA's Certification Practice Statement, Certificate Policy and associated policies, as amended from time to time by that Public CA (collectively "Public CA Policies"). The Public CA Policies can be consulted on-line at the web address indicated in the Order or can be obtained upon request. Customer shall operate and administer the RA in conformity with (i) the Public CA Policies, and (ii) such reasonable guidelines and/or instructions as Provider may inform Customer of from time to time.

57.1.4 By submitting a request to issue, suspend, re-instate or revoke a Certificate, Customer represents that (i) such request relates to an Authorized User; (ii) such request is submitted in compliance with Customer's own established application, validation and approval policies and procedures applicable to the RA, which shall not be inconsistent with or less stringent than the relevant Public CA Policies. Customer acknowledges and agrees that any request submitted on behalf of Customer to issue, suspend, re-instate or revoke a Certificate constitutes sufficient cause for Provider to honor such request.

57.2 Administration

57.2.1 Customer is responsible for appointing and authorizing only suitably skilled, trusted and qualified administrators to operate as RA on Customer's behalf ("Administrator"). Customer shall advise each Administrator of his or her obligations and Customer's obligations under this Section 57 and shall be responsible for each Administrator's knowledge, understanding, agreement and compliance therewith.

57.2.2 Unless otherwise agreed by Provider, at least two (2) and a maximum of four (4) Administrators must be appointed and registered with Provider at all times. Customer shall promptly inform Provider in writing of any change in the appointment and/or authorization of any of its Administrators.

57.2.3 Only an Administrator may request the issuance, suspension and/or revocation of Certificates and only via the web-based interface ("Administrator Interface") made accessible to Customer by Provider. Provider will provide each Administrator with an Administrator Certificate to access the Administrator Interface. Customer shall take commercially reasonable measures to prevent the compromise of the private keys associated with the Administrator Certificates and shall promptly inform Provider upon suspicion of or actual compromise of such private keys. Customer shall be liable for all activities and charges incurred through the use of the Administrator Certificates.

57.2.4 Customer, in its capacity as RA, acknowledges and agrees that it is responsible for collecting, proofing and recording each Authorized User's and each Administrator's personal data and any information to be entered into the Administrator Certificate.

57.2.5 Customer will indemnify and hold harmless Provider for and against all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Provider to the extent resulting from (i) any inaccuracy or error in the proofing and validation of the personal data or in any information to be entered into the Administrator Certificates and any other Certificates requested by Customer to be issued hereunder; (ii) the use or misuse of the Administrator Interface by an Administrator; and (iii) the use and/or compromise of an Administrator Certificate, except in so far as it can be shown that such liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) arise solely from Provider's negligence or willful misconduct in complying with its obligations and undertakings hereunder.

57.3 Services

57.3.1 As more fully described in the Order, Provider will provide the following CorporateSSL services to Customer:

57.3.1.1 Provide access to the Administrator Interface and provide the agreed number of Administrator Certificates as well as a set of Cybertrust branded certificate enrollment pages.

57.3.1.2 Have Certificates issued, revoked, re-instated and/or suspended from the Public CA's certificate services platform subject to an Administrator's request.

57.3.1.3 Provide, to Administrators only, first line technical support for queries regarding the Administrator Interface and reasonable second level technical support for queries related to an Authorized User's Certificate.

57.3.2 Customer shall comply with its responsibilities described in Section 57.3.6 below. In addition, Customer shall use commercially reasonable efforts to provide first line support to its Authorized Users. First line support includes the analysis and resolution of general queries regarding the installation and usage of the Certificates. To that end Customer agrees to regularly consult and stay current with the Public CA's Knowledge Base provided at the online support center location indicated in the Order. If, notwithstanding Customer's reasonable efforts, technical issues with a Certificate cannot be resolved, Customer, through Administrators only, may request second line support from Provider via the online support center at the location indicated in the Order.

57.3.3 Provider will make such training documentation available to Customer that Provider deems appropriate to familiarize the Administrators with the Administrator Interface and the administrative procedures relevant to the issuance, suspension and revocation of certificates. Customer can request additional training. One (1) such training will be provided free of charge over the internet (or through such other means of telecommunication available to Provider) and Customer shall cause its Administrators to attend such training. All additional training and documentation will be subject to availability and payment of additional fees. Additional training shall be provided on-site at Provider's offices or remotely via such telecommunication means as may be available at Provider's offices (e.g. conference call). In the event Customer and Provider agree to provide training at another location, all reasonable travel and expenses incurred by Provider shall be borne solely by Customer.

57.3.4 Provider enrolls, configures, and installs CorporateSSL for an annual fee. This fee includes the service establishment, operation, certificate verification services, SSL server certificates and support. Following initial establishment, Provider will perform ongoing certificate verification procedures and Certification Authority ("CA") maintenance. Certificates are purchased on a per-server, per-domain, or wildcard basis. Within the per-server model, if https://www.your-company-name.com is hosted on 10 separate Web servers, then these servers will consume 10 SSL certificates. Wildcard certificates have technical attributes that allow them to protect multiple servers, and they contain an * character at the beginning of the name meaning any name in that placeholder is acceptable. The following table describes the CorporateSSL service features and platform configuration:

| CorporateSSL Service | |
|---|---|
| **Delivery** | Installation after execution of Amendment 54 and Customer's provisioning of the required service enrolment information. |

| | |
|---|---|
| **Root** | Trusted Root CA, pre-installed in major browsers. |
| **End-entity certificate** | At least 1024 bit key, one, two or three-year validity period as requested. |
| **Certificate renewal issuance** | Certificate renewal / re-issuance with notification. |
| **Web Interface** | 1. Web-based publicly accessible enrolment pages receive requests from end users.<br>2. WebConnect Web-based registration authority. An authenticated portal operated by Customer's Registration Authority (RA) administrators to submit certificate requests and approve, reject, revoke and manage certificates. |
| **Certificate Application** | Standard fields will be provided for certificate content and authentication. These include details about the certificate content, the organization that is requesting the certificate, and the administrative and technical contacts that are responsible for the certificate. |
| **Authorization Method** | Manual approval of certificate requests via the RA interface. Client authentication digital certificates required for login for a minimum of 2 RA administrators are included. |
| **Certificates** | The certificates will be SSL server certificates with key usage marked for signing, key encipherment, non-repudiation and data encipherment.<br>The Distinguished name field requires the use of name, country, company name, and organizational name.<br>Option to purchase additional certificates or domains in blocks in accordance with price schedule. |
| **Certificate Revocation List** | The WebConnect Registration Authority interface revokes end-entity certificates. CRLs (Certificate Revocation Lists) are generated every three (3) hours. CRLs are available for download through WebConnect or from the web-site (currently http://crl.omniroot.com) as referred to from the CRL Distribution Point (CDP) extension within the certificate. |

57.3.5 Provider will deliver the following in support of the CorporateSSL platform:

57.3.5.1 Interactive Web Support – enables Customers to log on-line queries or issues. On submission, the Customer will be assigned a reference number that can be used to track the progress of the logged issue.

57.3.5.2 E-mail assistance – Customer can e-mail Provider's designated support desk with support queries.

57.3.5.3 Knowledge Base – Provider's on-line knowledge base enables Customer to access a repository of technical data to retrieve information on resolving known issues that may arise at Customer site.

57.3.6 The following chart outlines the responsibilities of the parties:

| PROVIDER | CUSTOMER |
|---|---|
| **SET-UP** | |
| | Complete Order Form to service agreement and submit to Provider (including domains for pre-verification and RA administrators' information). |
| Establish certificate service profile. | |
| Provide URLs for user-accessible WWW certificate enrollment pages and RA-only accessible WWW pages. | |
| Maintain an on-line database, which is kept at the Hosting Facility, of all currently valid certificates. | |
| **AUTHORIZATION METHOD AND APPROVAL PROCESS** | |
| Establish the Customer's Registration Authority (RA). | Establish the Customer's Registration Authority (RA). |
| | Notify the RA Administrators designated and appointed by the Customer to apply for an RA Administrator certificate and to perform the RA functions on Customer's behalf. |
| | Register the RA with Provider. |
| Issue RA Administrator certificates, on behalf of the Customer, to the RA Administrators authorized by the Customer, to allow for access by the RA Administrators to the RA-only accessible WebConnect WWW pages for purposes of performing RA functions. The Customer may not allow the RA Administrators to use the RA Administrator certificate for any other purpose. | |
| Provide the ability to access, review, update, and accept or reject certificate applications using the appropriate links on the WebConnect portal. | |
| | Review in a timely fashion all applications for certificates made available through the RA-only accessible WWW pages. Authenticate each applicant, verify the accuracy of the information supplied by the applicant, approve or reject the application. |
| | Require that RA(s) Administrators restrict access to the RA Administrator certificate(s), the private key associated with the RA Administrator certificate(s), and any user ID or password related to the RA Administrator certificates or the RA Administrator's right to access the RA-only accessible pages established at the WebConnect Portal. |
| **HARDWARE AND SOFTWARE MAINTENANCE** | |
| Operate the WebConnect Services WWW Site from the Hosting Facility. | |

| PROVIDER | CUSTOMER |
|---|---|
| Supply user-accessible pages, which are located at the WebConnect Services WWW Site that will be used for applying for end-user (server) certificates. Receive requests for server certificates in the form of a PKCS #10 certification request format. | |
| Deliver server certificates over a Web interface. Issue certificates with a validity period of 1, 2 or 3 years as specified in the Order. Make certificates available for retrieval after authorization of the application. | |
| Make the current status (active, revoked, expired) of a certificate available to the RA via an HTML interface. | |
| Renew/re-issue certificates upon Customer's request. | |
| | When the need arises to revoke a certificate immediately online through the RA, use the WebConnect portal to change the certificate status in the Customer Database to indicate the certificate has been revoked. |
| Revoke certificates by updating the status record in the Customer Database upon receipt of the appropriate direction from within the WebConnect portal. | |
| | Perform required due diligence to validate that all certificates issued are fully authorized and are only for domains authorized. |
| Periodically generate a Certificate Revocation List (CRL) for the Customer and make it constantly available for download through CRL Distribution Point extensions contained in the issued certificates. | |
| **NOTIFICATION OF A CHANGE OR COMPROMISE** | |
| | Notify Provider in the event any RA Administrator ceases to be an authorized RA Administrator, any information contained in an RA Administrator certificate changes or becomes false or misleading, or the private key corresponding to the public key contained in any RA Administrator certificate is compromised or likely to be compromised. |
| | Create a record of, and report to Provider, all actual or suspected compromises of the RA function and of any private keys as soon as the compromise is detected. |
| **MANAGEMENT SERVICES** | |

| PROVIDER | CUSTOMER |
|---|---|
| Maintain records of data related to the WebConnect WWW service, including security and audit data (three (3) years from generation), data concerning physical access to Customer-related material located in the Hosting Facility (1 year from date of access), and certificates (3) years from the earlier of revocation or expiration). | |
| Back up the operational Certificate Management System on a daily basis. | |
| Record certificate lifecycle management events. | |
| **SERVICE AVAILABILITY / SUPPORT - MAINTENANCE** | |
| Provide service availability and support as described in this Section 57. | |
| | Act as the sole intermediary for all communications with end users with the exception of access to the end user accessible WWW pages provided by the WebConnect service. |
| **FACILITY SECURITY** | |
| Maintain a secured facility audited against the Webtrust for CA accreditation scheme. | |

57.4

57.4.1 Provider reserves the right to revoke a Certificate at any time without notice and without indemnity or other liability upon occurrence of any or all of the following:

57.4.1 a revocation request issued by or on behalf of Customer;

57.4.2 Provider has good faith reasons to believe that the Certificate is or is likely to become compromised or used in an illegal or otherwise unauthorized manner;

57.4.3 Provider has good faith reasons to believe that any of the information contained in the Certificate has materially changed or is no longer accurate;

57.4.4 the Certificate has been issued to persons or organizations that are or at any time become identified or known as publishers of malicious software, or that impersonate other persons or otherwise undertake activities that are illegal, fraudulent or unethical;

57.4.5 any compelling event under applicable law (including, by way of example, if the Certificate has been issued to persons or organizations against which any form of supra-national, international, or national trade embargo becomes enforced);

57.4.6 Provider obtains reasonable evidence that Customer violated any of its material obligations under this Section 57 or otherwise under law;

57.4.7 Provider discontinues for any reason its provision of public certification services or the trust associated with the certificate hierarchy under which the Certificate has been issued becomes compromised;

57.4.8 Customer fails to maintain any permits, approvals, rights or authorizations as required for the issuance and/or use of the Certificate (including, without limitation, any failure to maintain domain name registration);

57.4.9 Provider determines that the Customer has engaged in activities that may be harmful or compromise Provider's (or Provider's affiliates', agents' or service providers') business reputation or status; or

57.4.10 Any additional and reasonable grounds for revocation as published from time to time in the Public CA Policies or otherwise made known to Customer.

Except as mandated by the Public CA Policies or applicable law, Provider does not have any obligation to revoke a Certificate upon occurrence of any or all of the events listed under Sections 57.4.1 through 57.4.10. Customer agrees that this Section 57.4 is without prejudice to and does not release Customer from its obligation to promptly request revocation of any Certificate upon learning or suspecting that any of the events pursuant to which Provider may revoke the Certificate has occurred or is likely to occur.

57.4.2 Upon revocation or expiration of a Certificate, Customer must permanently remove that Certificate from all applications, systems and/or devices on which it is installed and immediately cease all further use of the Certificate. If, in connection with the Certificate issued, Customer received a license from Provider to display a seal, logo, mark and/or other indicia on a website or other medium, Customer must immediately remove such seal or indicia upon revocation or expiration of the Certificate.

57.5 Fees and Payment

57.5.1 Customer shall pay Provider the fees reflected below, which fees will be stated in the Order. All amounts due for Corporate SSL services will be paid in accordance with the payment schedule set forth in the Order.

| *Service* | *One (1) Year* | *Two (2) Years* | *Three (3) Years* |
|---|---|---|---|
| SSL Web Server | $100.00 | $180.00 | $245.00 |
| SSL Web Server EV | $400.00 | $720.00 | N/A |
| SSL Wildcard | $300.00 | $540.00 | $735.00 |
| Code Signing Certificate | $100.00 | $180.00 | $245.00 |

57.5.2 Customer is solely responsible for any and all taxes or duties arising from or imposed on any CorporateSSL services delivered hereunder or amounts payable hereunder, excluding taxes based on Provider's net income. Without limiting the foregoing, Customer shall pay such additional amounts as may be required in order that the net amount actually received by Provider, after deduction or withholding of all applicable taxes and duties, shall be equal to the amount expressed to be payable pursuant to the terms of this Section 57 and the applicable Order(s).

57.5.3 Except to the extent otherwise agreed upon in the Order, Provider may revise its prices upon providing written notice to Customer at least ninety (90) calendar days prior to each Renewal Term of the Order anniversary date of the Order (as further defined in section 57.6.2 below). Such revised fees will take effect upon the Renewal Term of the Order unless Customer provides written notice to Provider in accordance with Section 57.6.2 below.

57.6 Term and Termination

57.6.1 Either party may terminate this Section 57 by written notice to the other party following the expiration or termination of its obligations under the Orders(s) executed hereunder.

57.6.2 The effective date and the initial term ("Initial Term") of each Order shall be as set forth therein.

57.6.3 Unless otherwise stated in the Order Form, following the Initial Term, the Order will be automatically renewed for subsequent equal periods (each a "Renewal Term") unless either party serves written notice of non-renewal to the other party at least sixty (60) calendar days prior to the end of the Initial Term or the then-current Renewal Term.

57.6.4 An Order may be terminated upon providing written notice (i) by either party, if the other party commits a material breach of any of its obligations thereunder and (if that breach is capable of remedy) fails to remedy it within thirty (30) calendar days of receipt of written notice thereof; (ii) by either party, if the other party ceases doing business, becomes insolvent or is affected by bankruptcy, liquidation or any similar procedure; (iii) by either party if the other party suffers a Force Majeure event (as defined in the Agreement) and such event persists for (1) calendar month or more; (iv) by Provider, if Provider's reputation, goodwill and/or infrastructure security posture is compromised or threatens to be compromised due to any act of failure to act by Customer. It will not be possible to manage any certificates that have been issued, or issue any further certificates or certificate revocation lists, once the applicable Order is terminated.

57.6.5 Upon termination or expiration of all Orders executed hereunder (i) the rights and licenses granted thereunder to Customer shall immediately terminate; (ii) Customer shall promptly cease all further use of the CorporateSSL services; (iii) the Administrator Certificates shall be revoked; (iv) each party shall promptly return to the other all proprietary and/or confidential material in its possession or under its

control and received from the other party under this Section 57, including all copies thereof. Termination or expiration of an Order shall not affect the continuance in force of any provision which is expressly or by implication intended to continue in force on or after such termination or expiration.

57.6.6 Upon termination or expiration of the Agreement (i) the rights and licenses granted hereunder to Customer shall immediately terminate; (ii) the Administrator Certificates shall be revoked and access to the Administrator Interface disabled; (iii) Customer shall discontinue all representations or statements on being a Provider appointed RA; (iv) Provider shall have the right to revoke any Certificate but no sooner than three (3) calendar months (or such other period of time mutually agreed upon in writing) following the effective date of termination or expiration of the Agreement; (v) no refund, credit or any other form of re-imbursement will be made in respect of any Certificates previously purchased, irrespective of such Certificates having been issued or not upon the effective date of termination or expiration of this Agreement; and (v) each party shall promptly return to the other all proprietary and/or confidential material in its possession or under its control and received from the other party under this Section 57, including all copies thereof. Termination or expiration of this Section 57 shall not affect the continuance if force of any provision which is expressly or by implication intended to continue in force on or after such termination or expiration. It will not be possible to manage any certificates that have been issued, or issue any further certificates or certificate revocation lists, once this Section 57 is terminated.

57.7 Data Protection and Confidentiality

57.7.1 I its performance hereunder each party shall comply with the applicable laws and regulations on data privacy and protection.

57.7.2 Notwithstanding the above, Customer agrees that, to the extent reasonably required to perform, administer, bill or account under this Section 57, Provider shall have the right to use, process and transfer any information and data obtained from or through Customer and disclose the same to Provider's employees, agents, professional advisers, subcontractors and affiliated companies, both in and outside one or more national or supra-national jurisdictions but solely in connection with its performance under the Section 57.

57.7.3 Customer represents and warrants that all concerned individuals and entities have given their consent to allow Provider to use, process and transfer their data as set forth herein and as required for the performance of CorporateSSL services.

57.7.4 In relation to the confidential and/or proprietary information that may be disclosed by or originate from a party hereto, the party receiving such information agrees to (i) limit access to such information to its officers, directors, employees and agents (including the officers, directors and employees of any related corporate body that controls, is controlled by or under common control with that party) who have a need to know such information for performance under this Section 57; (ii) use reasonable care and take reasonable measures to safeguard

the other party's confidential and/or proprietary information from inadvertent and/or unauthorized disclosure to any third party

57.8 All title, copyrights, trademarks, service marks, patents, patent applications and all other intellectual proprietary rights now known or hereafter recognized in any jurisdiction ("IP Rights") in and to the Provider's and Public CA's technology, web sites, documentation, products and services and any derivative works thereof ("Proprietary Materials") are, as between Provider and Customer, owned and will continue to be solely and exclusively owned by Provider. Customer agrees to make no claim of interest in or to any such IP Rights. Customer acknowledges that no title to the IP Rights in and to the Proprietary Materials is transferred to Customer and that Customer does not obtain any rights, express or implied, in any Proprietary Materials other than the rights expressly granted in this Section 57.

57.9 Provider warrants that the information embedded in each Certificate will, at the time of provisioning, contain no material errors as compared to the information provided by Customer resulting from Provider's or the Public CA's failure to exercise reasonable care in generating such Certificate. EXCEPT TO THE EXTENT EXPLICITLY STATED OTHERWISE IN THIS SECTION 57 AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, ALL PRODUCTS AND SERVICES ARE PROVIDED "AS IS" AND PROVIDER MAKES NO WARRANTIES WITH RESPECT TO USEFULNESS, FUNCTIONALITY, OPERABILITY, TIMELINESS AND NON-INFRINGEMENT. PROVIDER HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

57.10 Liability

57.10.1 PROVIDER'S AGGREGATE LIABILITY TO CUSTOMER FOR ALL DAMAGES AND IN RESPECT OF ANY AND ALL CAUSES OF ACTION AND CLAIM AT ANY TIME OR TIMES, INCLUDING, WITHOUT LIMITATION, ANY BREACH OF WARRANTY, SHALL NOT EXCEED AN AMOUNT TO THE LESSER OF (I) THE FEES ACTUALLY PAID BY CUSTOMER UNDER THIS SECTIOM 57 DURING THE PRECEDING TWELVE (12) MONTHS; AND (II) THE EQUIVALENT OF TWO-HUNDRED AND FIFTY THOUSAND U.S. DOLLARS ($250,000.00).

57.10.2 UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT OR OTHERWISE SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL SPECIAL, INDIRECT OR INCIDENTAL DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS, DATA, REVENUE OR INFORMATION, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

57.10.3 Customer shall bear sole and exclusive responsibility and liability to Provider and to any other entity and person for any actions or failures to act by Customer (including, without limitation, the acts or omissions by any Administrators) in connection with this Section 57.

57.10.4 The provisions of this Section 57.10 shall be enforceable to the maximum extent permitted by applicable law.

57.11 Customer shall keep reasonable records relating to any of Customer's responsibilities and obligations under this Section 57. During the term of the Agreement and for a period of (1) calendar year thereafter, Provider may, upon reasonable notice and during normal business hours, periodically audit Customer's compliance with these terms. In the event any such audit discloses any material breach by Customer (or its employees or agents) of its obligations hereunder, Customer shall, in addition to such other rights and remedies that may be available to Provider, refund Provider the reasonable costs and expenses incurred by Provider in connection with such audit.

57.12 Resale of the CorporateSSL services or Certificates is not permitted.

57.13 This Section 57 (including any Order) constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties with respect to the subject matter hereof. Provider's acceptance of a Customer purchase order ("P.O.") is for the sole purpose of facilitating Customer's payment procedures. All CorporateSSL services furnished in conjunction with a P.O. shall be governed solely by the terms and conditions of the Agreement and this Section 57. The terms of the Agreement and this Section 57 shall supersede and replace any terms and conditions contained in the P.O. and such terms and conditions shall not modify the Agreement and shall not be binding on Provider.

57.14 Each party agrees to comply with all applicable export laws and regulations. Customer shall not solicit and shall not accept any Certificate applications from any person or organization that is on the most recent United States export exclusion lists, and shall not perform any related functions (in whole or in part) in any country subject to any United Nations, USA, Australia or European Union embargo, regulation, terrorist controls or other similar restriction. Customer represents and warrants that any Authorized User is not located in, under the control of, or a national or resident of any such country or on any such list.

57.15 For the purposes of this Section 57, the following phrazes, terms and acronyms shall have the following meaning:

| | |
|---|---|
| Certificate Revocation List (CRL) | A data structure specified in ITU-T Recommendation X.509 that enumerates certificates which have been invalidated by their issuer prior to the time the certificate is scheduled to expire. |

| | |
|---|---|
| Certificate | A digitally signed document that is a public-key certificate in the version 1 or 3 format specified by ITU-T Recommendation X.509. The digital signature on the certificate binds a subject's identity and other data items to a public key value, thus attesting to the ownership of the public key by the subject. The certificate data items include, at least, the identity of the subject; the public key value; the identity of the certification authority that signs the certificate and the certificate's serial number. For the purpose of this Section 57, the term "certificate" includes administrator certificates, server certificates, and registration authority certificates. Certificates are sometimes referred to as "Customer certificates" or may be part of the definition of services. |
| Certification Authority (CA) | An entity that issues certificates and vouches for the binding between the data items in a certificate. |
| Customer Database | An online database that is maintained and controlled by Provider and which contains a copy and the status of all certificates. |
| Certificate Management System (CMS) | Provider's proprietary certificate management system, which provides the functions and capabilities that comprise WebConnect. |
| Hosting Facility | The site of Provider's secure facility in which the Certificate Authority system is located to provide WebConnect services |
| Private key: | The secret component of a key pair used for public-key (asymmetric) cryptography. The private key is kept secret by its owner and is used in conjunction with a matching, mathematically related public key. The key pair's owner uses the private key to sign data, or to decrypt data that was encrypted using the public key. Other parties use the matching public key to verify those digital signatures or to encrypt data to be sent to the owner of the public key. |
| Public key | The publicly disclosable component of a key pair used for public-key (asymmetric) cryptography. See private key. |
| Registration Authority (RA) | A public-key infrastructure entity, including those persons authorized to act on behalf of the entity, that performs authentication and verification functions (especially for the identities and other attributes of subjects) for applications for certificates and approves the issuance and revocation of certificates (and the performance of other certificate management functions). Under WebConnect, the Customer acts as the RA. |

| | |
|---|---|
| Secure Sockets Layer (SSL) | An Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented, end-to-end encryption to provide data confidentiality service and data integrity service for traffic between a client (a World Wide Web browser) and a server (a World Wide Web server). |
| Server certificate | Server certificate: A certificate issued to, and usually installed in a Web server to support transactions that use the Secure Sockets Layer (SSL) protocol. |
| Webtrust for CA accreditation scheme | The WebTrust Seal of assurance for Certification Authorities (CA) symbolizes to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria. Please see http://www.webtrust.org for more information. |
| WebConnect World Wide Web (WWW) Site | The WWW site that is established by Provider during activation of WebConnect. |
| WebConnect: | The services described in this Section 57 and the Orders. WebConnect is the RA administrator user interface. |