



Wealth Access Security Overview

Wealth Access is committed to taking all reasonable efforts to secure the personal data that we collect on our platform. To protect the privacy of any personal data, Wealth Access employs industry-standard physical and logical access controls, including but not limited to internal and external firewalls, intrusion detection, anti-virus protection, network monitoring and cryptographically strong methods when transmitting data.

Software Security

Wealth Access follows industry best practices while developing, testing and deploying our software. All custom or test accounts are removed prior to deployment. All code is peer-reviewed prior to promotion to release candidate. Wealth Access checks for common vulnerabilities such as SQL injection, buffer overflows, poor error handling and cross-site scripting prior to deploying software in our production environments.

Restrict access to data

Wealth Access limits the access to customer information by our employees to only those employees that require personal information to perform their job duties. The assignment of privileges is based on our employee's role in our organization. Wealth Access maintains a physical record of all visitors to our corporate offices.

Firewall

Wealth Access follows industry best practices for firewall and router configurations for local and remote servers. We employ a formal firewall change control policy and test all changes prior to implementation in production environments. Connections between trusted and untrusted connections are restricted. Reviews of our firewall rule sets are performed on a regular basis.

Encryption

Wealth Access utilizes strong cryptography during the transmission of all user information. Wireless networks and networking devices are secured following industry best practices prior to deployment in our corporate networks..

Virus Protection

All computers at Wealth Access have anti-virus software installed in order to protect against spyware and malware. Anti-virus protection is kept up to date according to vendor release cycles.

System Patching

All employee computers are patched from known vulnerabilities with vendor supplied patches. All patches are installed within a month of their availability. Wealth Access has an established process for ranking and patching critical vulnerabilities.

What data does the Wealth Access platform store?

During the onboarding process we ask for account and login information for various financial assets and holdings. This information is not stored on Wealth Access servers at any time. We only store this information with our trusted 3rd party technology partners.

Is my data secure at Wealth Access?

By employing industry-standard protocols for collecting and storing data, Wealth Access is committed to keeping your information private. All information that we store is read-only, there is no ability to modify your account information, execute trades or initiate transactions in anyway.

Do you store my account login information?

Account login information is not stored on our servers. We securely transmit your account information to our 3rd party vendors, who store your information in order to aggregate financial information.

What safeguards do you have in place to protect my information?

Information that we gather is encrypted during transmission. We do not store credit card or account information in our databases. Personal information that we store in our databases is encrypted at hosted sites that have achieved PCI DSS Level 1 certification.

Who are Wealth Access's 3rd party vendors?

<http://www.byallaccounts.com/privacy.html>

<http://www.yodlee.com/privacy-policy/>

<http://www.authorize.net/company/privacy/>

<http://aws.amazon.com/security/>

Privacy Policy

Wealth Access establishes a completely private and secure relationship between the company and the end user. The company works with the end user to establish their access to the platform. The end user remains in complete control of their Personal Identifiable Information.

The end user then grants access to view the information to a wealth advisor or anyone else he or she so chooses.

- The relationship is between the client and Wealth Access.
- All data is accessed in a read only format, nobody has the ability to take any action (buy/sell securities, transfer funds, bill payment, etc).
- Wealth Access does not store any credentials (user ids, passwords, etc.) on our servers. The client is responsible for entering and maintaining all credentials.
- Wealth Access does not market to investors.
- Wealth Access does not provide advice.
- Wealth access does not rent, sell or license the data to anyone.

Wealth Access legal counsel has fully reviewed and vetted this information. We are aware of all SEC, FINRA, and other laws and abide by those laws.

The third-party relationships that allow for the platform to provide accurate financial information for the clients are with the following vendors:

- Yodlee
- By All Accounts
- Amazon Web Services

Attached are sample agreements for both the end user and the private wealth advisor. Also, an overview of the security policy agreed to by Wealth Access and the above listed third party vendors. We are legally prohibited from sharing the signed agreements in their entirety.

Table of Contents

General Terms and Conditions: End User	5
General Terms and Conditions: Advisor Agreement.....	11
Yodlee: Privacy and Security FAQ.....	26
byallaccounts: Security & Privacy.....	30
Amazon Web Services: Security and Privacy.....	32

General Terms and Conditions: End User

These terms of service govern your use of the software and services available at wealthaccess.com (the “Platform”). Please read these Terms of Service carefully. By using the Platform, you are confirming that you have read and understand, and agree to be bound by, these Terms of Service. If you do not agree to these Terms of Service, you may not use the Platform.

Platform Access

Wealth Access, Inc. (“Wealth Access”) hereby grants you permission to use the Platform as set forth in these Terms of Service, provided that: (i) your use of the Platform as permitted is solely for your personal, noncommercial use in connection with your Wealth Access Account; (ii) you will not use the Platform in any way that is unlawful, misleading, malicious, or discriminatory; (iii) you will not do anything that could disable, overburden, or impair the proper working of the Platform (such as a denial of service attack); and (iv) you will otherwise comply with the terms and conditions of these Terms of Service.

You may not:

- access, tamper with, or use non-public areas of the Platform, Wealth Access’s computer systems, or the technical delivery systems of Wealth Access’s providers;
- attempt to probe, scan, or test the vulnerability of any system or network or breach any security or authentication measures;
- interfere with, or attempt to interfere with, the access of any user, host, or network, including, without limitation, sending a virus, overloading, flooding, spamming, or request-bombing the Platform;
- impersonate or misrepresent your affiliation with any person or entity;
- violate any local, state, national or international law or regulation;
- transmit any material that is fraudulent, abusive, harassing, tortious, defamatory, vulgar, pornographic, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically, or otherwise objectionable.

Wealth Access Account Requirements

In order to use the Platform, you will have to create an account.

Wealth Access Accounts are only available to users age 18 and older.

By registering with Wealth Access, you represent that you are able to form a binding contract and are not a person barred by any laws from using the Platform.

You are not allowed to use another user’s Wealth Access Account.

You agree that you will be personally liable for and will pay any and all fees that are associated with your account’s use of the Platform.

When creating your Wealth Access Account, you must provide accurate and complete information. You agree to provide true, accurate, current and complete information about yourself in all required fields of the registration form. If any of your information changes, you agree to update your registration information as soon as possible. If Wealth Access suspects that your registration information is not complete, current, or accurate, or that you have otherwise violated these Terms of Service, your Wealth Access Account may be subject to suspension or termination, and you may be barred from using the Platform.

You are solely responsible for the activity that occurs on and in your Wealth Access Account, and you must keep your password secure. You may change your password at any time by updating your account settings. In addition, you agree to immediately notify Wealth Access of any unauthorized use of your password or any other breach of security. Wealth Access cannot and will not be liable for any loss or damage arising from your failure to secure your Wealth Access Account.

Wealth Access Services

You understand that Wealth Access is not providing any financial or investment advice. Wealth Access is a personal finance information management service that allows you to consolidate and track your financial information in your Wealth Access Account. Information in your Wealth Access Account may come from: (i) you; (ii) your investment advisor that you may give permission to provide information to your Wealth Access Account (but only to the extent that you authorize they may do so); or (iii) any accounts you may have that are maintained online by third party financial institutions, if you direct Wealth Access to retrieve information from those accounts. You understand and acknowledge that the information in your Wealth Access Account is only as accurate and up-to-date as the sources that provide the information. **YOU ASSUME ALL RISK ASSOCIATED WITH YOUR USE OF THE PLATFORM.**

Information from Third Party Sites

If you direct Wealth Access to retrieve your financial information from certain third party sites, you explicitly authorize Wealth Access to act as your agent in order to receive that information on your behalf. When you enter your login and password (or other access credentials) to any third party site, you explicitly represent and warrant that you have all necessary rights to authorize your Wealth Access Account to access the information on that site on your behalf. You also authorize Wealth Access to use third party services including without limitation, the Yodlee Aggregation SDK (<http://yodlee.com/solutions-developer-api-yodlee-aggregation.html>) and byallaccounts (<http://www.byallaccounts.com/index.html>) to access your information from third party sites, in accordance with their terms of service. You understand and acknowledge that Wealth Access has no control over the accuracy of the information provided by third party financial institutions.

Your Content

Your Wealth Access Account may enable you to transmit content you select to the Platform for hosting, display, and distribution via your Wealth Access Account (collectively "Your Content"). When you instruct your Wealth Access Account to access Your Content, you grant to Wealth Access and its affiliates, representatives, and assignees a non-exclusive, fully-paid, world-wide, transferable, royalty-free license, with the right to grant sublicenses, to display, store, transcode, transmit, reproduce, edit, modify, create derivative works, and reuse your Your Content (or any portions or derivative works thereof) for the purposes you authorize within your Wealth Access Account.

For more information on how Your Content and personal information is stored, shared, and distributed in your Wealth Account, see the Wealth Access Privacy Policy. If you have questions not addressed by the Wealth Access Privacy Policy, please email atinfo@wealthaccess.com.

Wealth Access reserves the right to reject, remove or modify Your Content in its sole and absolute discretion at any time.

You represent and warrant that:

You own all rights in Your Content or, alternatively, you have acquired all necessary rights in Your Content to enable you to grant to Wealth Access the rights in Your Content described herein; you have paid and will pay in full all license fees, clearance fees, and any other financial obligations, of any kind, arising from any use Your Content in the Platform; you are the individual named in your Your Content, or, alternatively, if you are an advisor who has been provided access to an individual's account, you have obtained all necessary permissions from the person named in the Content to enable your use of the Platform in accordance with these Terms of Service; access by the Platform of Your Content does not infringe the intellectual property rights, privacy rights, publicity rights, or any other legal or moral rights of any third party. You agree to keep all records necessary to establish that your Your Content does not violate any of the foregoing representations and warranties and to make such records available to Wealth Access upon Wealth Access's request.

Feedback

You further agree that Wealth Access and its affiliates are free to use for any purpose whatsoever, ideas, know-how, concepts, techniques, comments, criticisms, reports, or other feedback other than Your Content ("Feedback"), whether oral or written, that you may send to Wealth Access or its affiliates. You acknowledge and agree that you have no expectation of compensation or confidentiality of any nature with respect to this feedback.

Alert Disclaimer

You understand and agree that any alerts that you request in your account settings and that Wealth Access provides to you may be delayed or prevented for reasons that Wealth Access cannot control. Wealth Access can neither guarantee the delivery nor the accuracy of the content of any alert. You agree that Wealth Access is not liable for any delays, failure to deliver, or misdirected delivery of any alert; for any errors in the content of an alert; or for any actions taken or not taken by you or any third party in reliance on an alert.

Termination

If you violate any of these Terms of Service, your permission to use the Platform and your Wealth Access Account automatically terminate.

Modifications To The Wealth Access Platform

Wealth Access reserves the right to modify or discontinue the Platform with or without notice to you. Wealth Access shall not be liable to you or any third party should Wealth Access exercise its right to modify or discontinue the Platform.

Disclaimer Of Warranties

YOU EXPRESSLY AGREE THAT USE OF THE PLATFORM IS AT YOUR SOLE RISK. THE PLATFORM IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. TO THE FULLEST EXTENT PERMITTED BY LAW, WEALTH ACCESS AND ITS AFFILIATES EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE PLATFORM AND YOUR WEALTH ACCESS ACCOUNT (INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE OR PURPOSE, AND NON-INFRINGEMENT). WEALTH ACCESS AND ITS AFFILIATES MAKE NO WARRANTIES OR REPRESENTATIONS ABOUT THE ACCURACY OR COMPLETENESS OF CONTENT AVAILABLE ON OR THROUGH THE PLATFORM OR THE CONTENT OF ANY APPLICATIONS OR THIRD PARTY SERVICES THAT WORK WITH THE PLATFORM AND ASSUME NO LIABILITY OR RESPONSIBILITY FOR ANY:

ERRORS, MISTAKES, OR INACCURACIES OF CONTENT OR APPLICATIONS;
PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM YOUR ACCESS TO OR USE OF THE PLATFORM OR YOUR WEALTH ACCESS ACCOUNT;

ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS OR ANY AND ALL PERSONAL INFORMATION OR FINANCIAL INFORMATION STORED THEREIN;

ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM THE PLATFORM;

ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE WHICH MAY BE TRANSMITTED TO OR THROUGH THE PLATFORM BY ANY THIRD PARTY; AND

FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT POSTED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE ON OR THROUGH THE PLATFORM.

WEALTH ACCESS AND ITS AFFILIATES DO NOT WARRANT, ENDORSE, GUARANTEE, OR ASSUME RESPONSIBILITY FOR ANY PRODUCT OR SERVICE ADVERTISED OR OFFERED BY A THIRD PARTY THROUGH THE PLATFORM OR ANY LINKED SERVICE, APPLICATION, OR PLATFORM, AND WEALTH ACCESS AND ITS AFFILIATES WILL NOT BE A PARTY TO OR IN ANY WAY BE RESPONSIBLE FOR MONITORING ANY TRANSACTION BETWEEN YOU AND THIRD PARTY PROVIDERS OF PRODUCTS OR SERVICES. YOU UNDERSTAND AND AGREE THAT ANY MATERIAL OR INFORMATION DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE PLATFORM IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE ARISING THEREFROM. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM WEALTH ACCESS OR THROUGH THE PLATFORM SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN.

Limitation Of Liability

YOU UNDERSTAND THAT TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, IN NO EVENT WILL WEALTH ACCESS OR ITS OFFICERS, EMPLOYEES, DIRECTORS, SHAREHOLDERS, PARENTS, SUBSIDIARIES, AFFILIATES, AGENTS, OR LICENSORS BE LIABLE UNDER ANY THEORY OF LIABILITY (WHETHER IN CONTRACT, TORT, STATUTORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, DAMAGES FOR LOSS OF REVENUES, PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF SUCH PARTIES WERE ADVISED OF, KNEW OF OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM YOUR (OR ANYONE USING YOUR ACCOUNT'S) USE OF THE PLATFORM OR YOUR WEALTH ACCESS ACCOUNT.

Exclusions And Limitations

Some jurisdictions do not allow the exclusion of certain warranties or the limitation or exclusion of liability for incidental or consequential damages. Accordingly, some of the above limitations and disclaimers may not apply to you. To the extent Wealth Access may not, as a matter of applicable law, disclaim any implied warranty or limit its liabilities, the scope and duration of such warranty and the extent of Wealth Access's liability shall be the minimum permitted under such applicable law.

Indemnity

You agree to indemnify, defend, and hold harmless Wealth Access, its parents, subsidiaries, affiliates, officers, directors, employees, consultants and agents from and against any and all claims, liabilities, damages, losses, costs, expenses, fees (including reasonable attorneys' fees and costs) that such parties may incur as a result of or arising from (1) any information (including, without limitation, your Your Content, Feedback, or any other content) you (or anyone using your account) submit, post, or transmit on or through the Platform; (2) your (or anyone using your account's) use of the Platform; (3) your (or anyone using your account's) violation of these Terms of Service; or (4) your (or anyone using your account's) violation of any rights of any other person or entity, including, without limitation, any copyright, patent, trademark, trade secret or other proprietary rights of any person or entity. Wealth Access reserves the right, at its own expense, to assume the exclusive defense and control of any matter otherwise subject to indemnification by you, in which event you will cooperate with Wealth Access in asserting any available defenses.

Miscellaneous

Without limiting the foregoing, under no circumstances will Wealth Access be held liable for any delay or failure in performance due in whole in or in part to any acts of nature, forces, or causes beyond its reasonable control. In the event that any provision of these Terms of Service is held to be invalid or unenforceable, the remaining provisions of these Terms of Service will remain in full force and effect. The failure of Wealth Access to enforce any right or provision of these Terms of Service will not be deemed a waiver of such right or provision.

Controlling Law and Jurisdiction

These Terms of Service and any action related thereto will be governed by the laws of the State of Tennessee without regard to any conflict of laws principles or rules. The exclusive jurisdiction and venue of any action with respect to the subject matter of these Terms of Service will be the state and federal courts located in Davidson County, Tennessee, and each of the parties hereto expressly waives any objection to and agrees to submit to jurisdiction and venue in such courts.

Entire Agreement

These Terms of Service, together with the Wealth Access Privacy Policy, which is hereby incorporated by reference and any other rules or guidelines posted in connection with the Platform, are the entire and exclusive agreement between Wealth Access and you regarding the Platform and your Wealth Access Account. These Terms of Service supersede and replace any prior agreements between Wealth Access and you regarding the Platform.

Terms of Service Changes

Wealth Access may, in its sole and absolute discretion, change these Terms of Service from time to time. Wealth Access will post a copy of the Terms of Service as changed on the Platform. Your continued use of the Platform after the changed terms are posted constitutes your agreement to abide by the Terms of Service as changed. If you object to any such changes, your sole recourse shall be to cease using the Platform.

If you have any questions about these Terms of Service, please contact us at info@wealthaccess.com.
Last Revised: May 16, 2012.

[End of Agreement]

General Terms and Conditions: Advisor Agreement

The terms and conditions set forth below are an integral part of the Advisor License and Services Agreement entered into between Wealth Access, LLC, and Customer:

1. Certain Definitions.

“Advisor Dashboard User” means an employee of, or an individual independent contractor to, Customer or an Affiliate, in each case as authorized by Customer in accordance with Section 2(b) and pursuant to the provisions of Exhibit B, and in each such case so long as such authorization has not been canceled as contemplated in Exhibit B.

“Affiliate” means an entity that controls, is controlled by, or is under common control with Customer, “control” meaning possession, directly or indirectly, of a majority of an entity’s voting interests.

“Application” means the software application offered by Wealth Access on a hosted (software as a service) basis that provides tools to assist in the administration of investment portfolios, together with any associated database structures and queries, interfaces, tools, and the like as initially provided by Wealth Access to Customer pursuant to this Agreement, together with any and all revisions, modifications, and updates thereof, all as may be provided by Wealth Access to Customer pursuant to this Agreement.

“Confidential Information” means any information of any type in any form that (i) is disclosed to or observed or obtained by one party from the other party (or from a person the recipient knows or reasonably should assume has an obligation of confidence to the other party) in the course of, or by virtue of, this Agreement and (ii) either is designated as confidential or proprietary in writing at the time of such disclosure or within a reasonable time thereafter (or, if disclosure is made orally or by observation, is designated as confidential or proprietary orally by the person disclosing or allowing observation of the information) or is of a nature that the recipient knew or reasonably should have known, under the circumstances, would be regarded by the owner of the information as confidential or proprietary. For purposes of this Agreement, however, the term “Confidential Information” specifically shall not include any portion of the foregoing that (i) was in the recipient’s possession or knowledge at the time of disclosure and that was not acquired directly or indirectly from the other party, (ii) was disclosed to the recipient by a third party not having an obligation of confidence of the information to any person or body of which the recipient knew or which, under the circumstances, the recipient reasonably should have assumed to exist, or (iii) is or, other than by the act or omission of the recipient, becomes a part of the public domain not under seal by a court of competent jurisdiction. No combination of information will be deemed to be within any of the foregoing exceptions, regardless whether the component parts of the combination are within one or more exceptions. In the event of any ambiguity as to whether information is Confidential Information, the foregoing shall be interpreted strictly and there shall be a rebuttable presumption that such information is Confidential Information.

“Customer Data” means all data entered into the Application by Advisor Dashboard Users (other than data of an Investor entered by an Advisor Dashboard User on behalf of such Investor) or entered into the

Application by or on behalf of Customer pursuant to a conversion from or interface with another system, in either case as such data is maintained in the Application from time to time during this Agreement.

“Customer Property” means all tangible or intangible property (including without limitation Customer Data and intellectual property of any type) delivered to Wealth Access by or on behalf of Customer (other than payments) to facilitate Wealth Access’s performance of its obligations under this Agreement. Any of the foregoing delivered prior to the Effective Date in contemplation of this Agreement shall be deemed to be Customer Property.

“Data Provider” means a third-party engaged by Wealth Access to access, upon authorization by an Investor, investment account information from other third parties that maintain such accounts and to provide such information to Wealth Access.

“Documentation” means all documentation (whether printed or in an electronic retrieval format) supplied or made available to Customer by Wealth Access for use with or in support of the Application or its implementation, including without limitation any and all revisions, modifications, and updates thereof as may be supplied or made available by Wealth Access to Customer during the term of this Agreement and all copies thereof made by or on behalf of Customer.

“Environment Specifications” means the minimum information technology environment necessary for Use of the Application described in the FAQs published by Wealth Access on its web site at www.wealthaccess.com, as revised from time to time by written notice to Customer, a copy of which as of the Effective Date has been delivered to Customer.

“Fees and Expenses” means all fees, expenses, and other charges set forth in this Agreement to be paid by Customer, including without limitation the subscription fees and such other amounts, if any, as are described in Exhibit A.

“Infringement Claim” means a claim that Customer’s use of any Licensed Materials in accordance with the terms and conditions of this Agreement infringes a copyright or patent of a third party (other than an Affiliate) that is enforceable in the United States.

“Investor” means a Single-Portfolio Investor or a Multiple-Portfolio Investor.

“Investor Subscription” means a Single-Portfolio Investor Subscription or a Multiple-Portfolio Investor Subscription.

“License Counts” has the meaning ascribed in Exhibit A.

“Licensed Materials” means the Application and the Documentation.

“Malfunction” means a reproducible material failure of the Application to provide the operational functionality described in the Documentation.

“Multiple-Portfolio Investor” means a party that has entered into a subscription agreement with Wealth Access for use of the Application with respect to multiple Portfolios pursuant to authorization by Customer as contemplated in Exhibit B and as to such agreement with Wealth Access has not been terminated as provided therein or in this Agreement.

“Multiple-Portfolio Investor Subscription” means the right for an Multiple-Portfolio Investor to use the Application during the term of this Agreement in accordance with an agreement between such Investor and Wealth Access.

“Investor Dashboard User” means an individual designated as such by a Multiple-Portfolio Investor as contemplated in Exhibit B.

“Portfolio” means an a set of related investment accounts identified to Wealth Access by an Investor.

“Problem Report” means a written report delivered to Wealth Access by Customer describing a suspected Malfunction and identifying in reasonable detail the basis for such suspicion.

“Single-Portfolio Investor” means a party that has entered into a subscription agreement with Wealth Access for use of the Application with respect to a single Portfolio pursuant to authorization by Customer as contemplated in Exhibit B and as to such agreement with Wealth Access has not been terminated as provided therein or in this Agreement.

“Single-Portfolio Investor Subscription” means the right for an Single-Portfolio Investor to use the Application during the term of this Agreement in accordance with an agreement between such Investor and Wealth Access.

“Statement of Work” means an addendum to this Agreement duly executed by each party that sets forth requirements, pricing, acceptance methodology, fees, expense reimbursements, and other respective responsibilities of the parties as to implementation, customization, feature development, interface development, and other project services to be provided by Wealth Access to Customer pursuant to this Agreement; provided, however, that the failure of a Statement of Work to comply with the foregoing standards shall not, in itself, invalidate such Statement of Work.

“Use” means (i) accessing and operating the Application from a location within the United States in conjunction with the provision of financial or other professional services to Investors or for Customer’s internal business purposes in support of the foregoing, and (ii) reading of a copy of Documentation by a human (with or without the aid of a machine or device) in connection with accessing and operating the Application as provided herein.

2. License to Customer.

(a) License Grant. Subject to terms and conditions of this Agreement, Wealth Access grants to Customer a non-exclusive, non-transferable (except as otherwise provided herein) license during the term of this Agreement (i) for Use of the Application and Documentation by Advisor Dashboard Users in accordance

with the terms of this Agreement and (ii) to authorize third parties to enter Investor Subscriptions as set forth in Exhibit B.

(b) **Limitation on Access by Contractors.** Customer shall not authorize an independent contractor as an Advisor Dashboard User if, to the knowledge of Customer and its Affiliates, such person is employed by any other person or entity (other than a company engaged principally in recruiting and placing personnel) unless Customer has disclosed the identity of such employer and the nature of such relationship to Wealth Access and Wealth Access has approved such arrangement in writing in its sole discretion. Should Customer or any Affiliate discover any such other employment of a person already authorized as an Advisor Dashboard User, Customer immediately shall cancel such person's authorization as contemplated in Exhibit B unless otherwise agreed by Wealth Access in writing in its sole discretion.

3. **Services.** Subject to the terms and conditions of this Agreement, provided Customer is not in default of its obligations hereunder, Wealth Access shall provide, and Customer shall accept, the following services during the term of this Agreement:

(a) **Application Hosting.** Wealth Access will host the Application as software-as-a-service in a multi-tenant environment and make it available via the Internet for Use by Advisor Dashboard Users.

(b) **Application Support.** Subject to such terms and conditions as may be set described in Exhibit C, Wealth Access shall provide to Advisor Dashboard Users consultation and assistance with operational and technical support issues arising from Use of the Application. Customer's requests for support services shall be submitted by telephone or e-mail at such numbers and e-mail addresses as Wealth Access shall provide to Customer from time to time.

(c) **Application Maintenance and Enhancement.** In response to a Problem Report, Wealth Access shall use commercially reasonable efforts to correct a reported Malfunction or to provide a reasonable workaround sufficient to alleviate any material adverse effect of the problem on the utility of the Application, provided Customer assists Wealth Access in its efforts to correct a Malfunction by making available information, documentation, access to personnel, and testing reasonably requested by Wealth Access from time to time to assist Wealth Access in identifying and correcting the problem. In the event a Malfunction exists due to an error in Documentation, Wealth Access may correct such Malfunction by providing corrected Documentation; provided, however, that no revision, modification, or update to Documentation shall eliminate or materially diminish any operational functionality of the Application previously described therein. From time to time at its sole discretion, Wealth Access also may implement releases of the Application that contain changes, updates, patches, fixes, enhancements to functionality, and/or additional functionality. Wealth Access in its sole discretion will determine whether to include in the Application, as part of the maintenance services hereunder, features or functionality offered in other products that could be incorporated into the Application, and Wealth Access shall have no obligation to disclose or offer to Customer any such products, features, or functionality.

(d) **Other Services.** Wealth Access shall provide such other services as are described in Exhibit C or as agreed by the parties in a Statement of Work or other written agreement from time to time.

(e) Supported Environment. Wealth Access's support and maintenance obligations pursuant to this Agreement are conditioned on Use of the Application in an information technology environment meeting the Environment Specifications.

4. Customer Obligations.

(a) Customer Connection. Customer shall be responsible for selecting, obtaining, and maintaining any equipment, computer software, Internet access, and telecommunication or other ancillary services needed to connect to or otherwise access the Applications in accordance with the Environment Specifications.

(b) Logon Credentials and Data Security. Customer shall maintain or cause to be maintained the confidentiality of all Advisor Dashboard User logon credentials. Customer shall be solely responsible for all use or misuse of Advisor Dashboard User logon credentials. All Advisor Dashboard User logon credentials shall be deemed to be Confidential Information. CUSTOMER SHALL ENSURE THAT ITS PERSONNEL DO NOT SHARE LOGON CREDENTIALS OR ATTEMPT TO ACCESS THE APPLICATION WITHOUT PROVIDING VALID LOGON CREDENTIALS. Except with respect to the hosting services provided by Wealth Access, Customer shall be solely responsible for and shall maintain, in connection with the operation of the Application, adequate technical, physical, and procedural access controls and system security requirements and devices, including without limitation causing each Advisor Dashboard User to use appropriately complex passwords and to change his or her password at such intervals and upon such circumstances as Customer deems appropriate and prudent or as directed or enforced by Wealth Access in its sole discretion. Wealth Access shall not be liable to Customer for, and Customer shall indemnify, defend, and hold harmless Wealth Access and its directors, officers, and employees from and against any loss, cost, or liability (including without limitation reasonable attorney fees and expenses) resulting from or relating to, Customer's failure to maintain its obligations set forth in this paragraph.

(c) Restrictions. Customer shall not do, nor shall it authorize any person do, any of the following: (i) use the Licensed Materials for any purpose or in any manner not specifically authorized by this Agreement; (ii) make any copies or prints, or otherwise reproduce or print, any portion of the Licensed Materials, whether in printed or electronic retrieval format, except as expressly provided in this Agreement; (iii) distribute, republish, download, display, post, or transmit any portion of the Licensed Materials except as explicitly authorized by this Agreement (by way of clarification, the production of reports generated by the Application shall not be deemed a violation of this clause); (iv) create or recreate the source code for any or all of the Application, or re-engineer, reverse engineer, decompile, disassemble, modify, or alter any or all of the Application except as may be expressly authorized in this Agreement; (v) modify, adapt, translate, or create derivative works based upon any part of the Licensed Materials, or combine or merge any part of the Licensed Materials with or into any other software, content, or documentation except as expressly authorized by this Agreement; (vi) refer to or otherwise use any part of the Licensed Materials in any effort to develop a program having any functional attributes, visual expressions, or other features similar to those of the Licensed Materials or to compete with Wealth Access except as may be expressly authorized by this Agreement; (vii) remove, erase, or tamper with any copyright, logo, or other proprietary or trademark notice printed or stamped on, affixed to, or encoded or recorded in the Licensed Materials, or fail to preserve all copyright and other proprietary notices in any copy (whether authorized

or unauthorized) of any portion of the Licensed Materials made by Customer; (viii) except as otherwise expressly provided by this Agreement, sell, market, license, sublicense, distribute, rent, loan, operate for, or otherwise provide to any third party any right to possess or utilize any portion of the Licensed Materials without the express prior written consent of Wealth Access (which may be withheld by Wealth Access for any reason or conditioned upon execution by such party of a confidentiality and non-use agreement and/or other such other covenants and warranties as Wealth Access in its sole discretion deems desirable); (ix) use the Licensed Materials to gain or attempt to gain unauthorized access to any applications or services for which Customer has not paid the applicable fees to use or any software or computer systems belonging to any third party that has access to the Application; or (x) attempt to do or assist any party in attempting to do any of the foregoing.

5. Fees and Expenses; Late Payments; Taxes. Customer shall pay all Fees and Expenses as provided in this Agreement. Without limiting any other obligations of Customer, in the event of termination of this Agreement, Wealth Access shall have no obligation to refund any Fees and Expenses paid by Customer for the month of termination. Payments not received within 30 days after the due date shall accrue interest from such due date at the rate of 1.5% per month or, if less, at the highest rate permitted by applicable law. Customer shall promptly reimburse all charges or penalties levied against Wealth Access for returned check fees or the like. Customer shall pay when due (and Wealth Access at its discretion may collect and pay on Customer's behalf) all taxes based on or in any way measured by this Agreement, the services provided hereunder, or Customer's use of the Licensed Materials or any portion thereof, excluding taxes based on Wealth Access's net income, but including without limitation sales and use taxes and personal property taxes, if any.

6. Ownership of Licensed Materials and Customer Data.

(a) Customer Property. As between Wealth Access and Customer, has and retains exclusive and valid ownership of all Customer Property.

(b) Licensed Materials. As between Wealth Access and Customer, Wealth Access has and retains exclusive and valid ownership of the Licensed Materials, the names and marks thereof, and all intellectual property and proprietary rights therein, and Customer acknowledges that the foregoing constitute valuable assets and may constitute trade secrets of Wealth Access.

(c) Suggestions and Joint Efforts. Customer may suggest, and the parties may discover or create jointly, findings, inventions, improvements, discoveries, or ideas that Wealth Access, at its sole option, may incorporate in the Licensed Materials or in other products or services that may or may not be made available to Customer. Any such finding, invention, improvement, discovery, or idea, whether or not patentable, that is conceived or reduced to practice during the term of this Agreement, whether by a party alone or by the parties jointly, arising from or related to this Agreement or the Licensed Materials shall be and remain the sole property of Wealth Access and may be used and be sold, licensed, or otherwise provided by Wealth Access to third parties, or published or otherwise publicly disclosed, in Wealth Access's sole discretion without notice, attribution, payment of royalties, or liability to Customer. Customer hereby assigns to Wealth Access any and all right, title, and interest, including without limitation copyright and patent rights, in and to any such findings, inventions, improvements, discoveries,

and ideas. Unless otherwise expressly agreed in writing, Customer shall not obtain any right, title, or interest in or to anything created or developed by Wealth Access in connection with or incident to this Agreement other than the license expressly set forth herein.

7. License to Use Customer Property. Customer grants to Wealth Access a non-exclusive, royalty-free license during the term of this Agreement to use and disclose Customer Property to perform its obligations under this Agreement and to use (but not disclose except as otherwise provided in this Agreement) Customer Data for purposes of (i) monitoring, improving, and correcting the performance of the Application, developing enhancements to the Application and new products, and other internal business purposes, (ii) compiling statistical information (including without limitation aggregating Customer Data with other data) that does not identify Customer or any Investor, and (iii) creating de-identified versions of Customer Data, which shall be owned by Wealth Access and may be used and disclosed for any lawful purpose during or after the term of this Agreement. Customer represents and warrants that (i) it owns or has the legal right and authority, and will continue to own or maintain the legal right and authority, to grant to Wealth Access during the term of this Agreement the license set forth in this paragraph and (ii) Wealth Access's use of Customer Property as provided herein will not infringe any intellectual property or proprietary right or violate any trade secret or otherwise violate any right of a third party. Customer shall indemnify, defend, and hold harmless Wealth Access and its directors, officers, and employees from and against any loss, cost, or liability (including without limitation reasonable attorney fees and expenses) arising from or relating to a claim of a third party with respect to a breach of the foregoing representations and warranties of Customer.

8. Backup Copies. Customer may make copies of such portions of the Documentation as are provided or made available by Wealth Access in an electronic retrieval format, provided that no more than a reasonable and necessary number of such copies of the Documentation may be in existence at any one time. Upon request from time to time, Customer shall notify Wealth Access in writing of the number of such backup copies and of the location(s) thereof. Customer shall preserve on and/or in all such backup copies all of Wealth Access's copyright and other restrictive and proprietary notices in the form and content as they appear on and/or in the Documentation. Customer acknowledges and agrees that all such backup copies are and shall remain Licensed Materials.

9. Confidentiality.

(a) Information Deemed Confidential. Without limiting any other provisions of this Agreement or granting by implication any rights with respect to any particular item, and whether or not otherwise meeting the criteria described herein, the following shall be deemed conclusively to be Confidential Information: (i) all information that is a trade secret of a party pursuant to applicable law; and (ii) to the extent not generally known to the public or to third parties in the relevant industry, all data, documents, flow charts, logic diagrams, design concepts, technical information, processes, standards, specifications, improvements, inventions, procedures, know-how, formulae, algorithms, source and executable codes, scripts, file layouts, database arrangements, test materials, business concepts and methods, financial information, sales and marketing information, development plans, business plans, strategies, forecasts, customer lists, customer data, and passwords, entry codes, access sequences, or the like of a party.

(b) Security of Confidential Information. In addition to any other restrictions or obligations imposed at law or provided under this Agreement, each party possessing Confidential Information of the other party will maintain all such Confidential Information under secure conditions, using reasonable security measures and in any event not less than the same security procedures used by such party for the protection of its own Confidential Information of a similar kind.

(c) Non-Disclosure Obligation. Except as otherwise may be permitted by this Agreement, neither party shall disclose any Confidential Information of the other party to any third party without the express prior written consent of the other party; provided, however, that either party may disclose appropriate portions of Confidential Information of the other party to those of its employees, contractors, agents, and professional advisors having a substantial need to know the specific information in question in connection with such party's exercise of rights or performance of obligations under this Agreement provided that all such persons (i) have been instructed that such Confidential Information is subject to the obligation of confidence set forth by this Agreement and (ii) are bound either by contract, employment policies, or fiduciary or professional ethical obligation to maintain such information in confidence.

(d) Compelled Disclosure. If either party is ordered by a court, administrative agency, or other governmental body of competent jurisdiction to disclose Confidential Information, or if it is served with or otherwise becomes aware of a motion or similar request that such an order be issued, then such party will not be liable to the other party for disclosure of Confidential Information required by such order if such party complies with the following requirements: (i) if an already-issued order calls for immediate disclosure, then such party immediately shall move for or otherwise request a stay of such order to permit the other party to respond as set forth in this paragraph; (ii) such party immediately shall notify the other party of the motion or order by the most expeditious possible means; and (iii) such party shall not oppose a motion or similar request by the other party for an order protecting the confidentiality of the Confidential Information, including not opposing a motion for leave to intervene by the other party; and (iv) such party shall exercise reasonable efforts to obtain appropriate assurance that confidential treatment will be accorded the Confidential Information so disclosed.

(e) Non-Use Obligation. Except as expressly authorized in this Agreement, during the term of this Agreement and forever thereafter (or for such shorter period as may be imposed by applicable law), neither party shall use any Confidential Information of the other party, except at the request of and for the benefit of such other party, without the express prior written consent of the other party.

(f) Copying of Confidential Information. Except as otherwise may be permitted by this Agreement, neither party shall copy or otherwise reproduce any part of any Confidential Information of the other party, nor attempt to do so, without the prior written consent of the other party. Any embodiments of Confidential Information of a party that may be generated by the other party, either pursuant to or in violation of this Agreement, will be deemed to be the sole property of the first party and fully subject to the obligations of confidence set forth herein.

(g) Proprietary Legends. Without the other party's prior written consent, neither party shall remove, obscure, or deface on or from any embodiment of any Confidential Information any proprietary legend relating to the other party's rights.

(h) Reports of Misappropriation. Each party immediately shall report to the other party any act or attempt by any person of which such party has knowledge or reasonably suspects (i) to use or disclose, or copy Confidential Information without authorization from the other party or (ii) to reverse assemble, reverse compile, or otherwise reverse engineer any part of the Confidential Information.

(i) Post-Termination Procedures. Except as otherwise provided in this Agreement, as soon as practicable upon any termination of this Agreement or other termination of a party's right to possess and/or use Confidential Information, each party shall turn over to the other party (or destroy and certify the same in writing) any embodiments of any Confidential Information of the other party.

10. Warranties; Disclaimers.

(a) Services. Wealth Access warrants that it will perform the services provided hereunder in a workmanlike manner using duly qualified and experienced personnel.

(b) Viruses. Wealth Access represents that to its knowledge the Application does not and will not contain any computer code designed to disrupt, disable, harm, or otherwise impede the operation thereof or of any associated software, firmware, hardware, computer system, or network (sometimes referred to as "viruses" or "worms") and warrants that it will take commercially reasonable efforts to ensure that no third party causes the same to be embodied in the Application.

(c) Data Providers. Customer acknowledges that the operation of the Application is dependent upon the services of certain Data Providers and that such data providers will receive, maintain, and transmit sensitive information, including without limitation authentication credentials and personal financial information, in the course of providing services to Wealth Access in furtherance of the operation of the Application. Wealth Access makes no representation or warranty with respect to, and expressly disclaims any responsibility for or liability arising from, any act or omission of a Data Provider, including without limitation any unauthorized use or disclosure of such sensitive information or the consequences thereof to Customer or any other person. Wealth Access does not warrant that it will utilize or continue to utilize the services of any particular Data Provider or that a Data Provider will provide or continue to provide access to the investment accounts maintained by any particular third party.

(d) WARRANTY DISCLAIMERS. THE EXPRESS WARRANTIES AND EXPRESS REPRESENTATIONS SET FORTH IN THIS AGREEMENT ARE IN LIEU OF, AND WEALTH ACCESS DISCLAIMS, ANY AND ALL OTHER WARRANTIES, CONDITIONS, OR REPRESENTATIONS (EXPRESS OR IMPLIED, ORAL OR WRITTEN), WITH RESPECT TO THE LICENSED MATERIALS OR ANY PART THEREOF OR THE SERVICES HEREUNDER, INCLUDING WITHOUT LIMITATION ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT WEALTH ACCESS KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR OTHERWISE IS IN FACT AWARE OF ANY SUCH PURPOSE), WHETHER ALLEGED TO ARISE BY LAW, BY REASON OF CUSTOM OR USAGE IN THE TRADE, BY COURSE OF DEALING, OR OTHERWISE. WEALTH ACCESS

EXPRESSLY DISCLAIMS ANY WARRANTY OR REPRESENTATION TO ANY PERSON OTHER THAN CUSTOMER WITH RESPECT TO THE LICENSED MATERIALS OR ANY PART THEREOF.

(e) Other Disclaimers. Customer will be exclusively responsible as between the parties for, and Wealth Access makes no warranty or representation with respect to, determining whether the Application will achieve the results desired by Customer, ensuring the accuracy of any data, and selecting, procuring, installing, operating, and maintaining the technical infrastructure for Customer's access to and use of the Application. Wealth Access shall not be liable for, and shall have no obligations with respect to, any aspect of the Application that is modified by any person other than Wealth Access or its contractors, use of the Application other than in accordance with the most current operating instructions provided by Wealth Access, malfunctions or failures caused by defects, problems, or failures of hardware or software not provided by Wealth Access, or malfunctions or failures caused by acts or omissions of Customer or any third party. Customer acknowledges that the operation of the Application will not be error free in all circumstances, that all defects in the Application may not be corrected, and that the operation of the Application may be interrupted for reasonable periods of time by reason of defect therein or by reason of fault on the part of Wealth Access. Due to the continual development of new techniques for intruding upon and attacking networks, Wealth Access does not warrant that the Application or any equipment, system, or network on which the Application is used or accessed will be free of vulnerability to intrusion or attack.

11. Intellectual Property Indemnification.

(a) Indemnity. Wealth Access shall indemnify Customer and its directors, officers, and employees against any final judgment entered in respect of an Infringement Claim by a court of competent jurisdiction and against any settlements arising out of such a claim. Wealth Access's obligations specified in this paragraph will be conditioned on Customer's notifying Wealth Access promptly in writing of the Infringement Claim or threat thereof (whether or not litigation or other proceeding has been filed or served) and giving Wealth Access full and exclusive authority for, and information for and assistance with, the defense and settlement of such claim and any subsequent appeal.

(b) Remedies. If an Infringement Claim has occurred or in Wealth Access's opinion is likely to occur, Customer agrees to permit Wealth Access, at its option and expense, either to (i) procure for Customer the right to continue using the Licensed Materials, (ii) replace or modify the same so that it becomes non-infringing, or (iii) immediately terminate both parties' respective rights and obligations under this Agreement with regard to the Licensed Materials, in which case, if the Customer possesses any Licensed Materials, Customer will return all copies thereof to Wealth Access and Wealth Access will refund to Customer the applicable license fees paid by Customer for the then-current term of this Agreement prorated for the portion of the term through the date of such termination.

(c) Exceptions. The foregoing notwithstanding, Wealth Access shall have no liability for, and Customer will indemnify Wealth Access and its directors, officers, and employees against, any claim arising from (i) the combination, operation, or use of any Licensed Materials with equipment, devices, or software not supplied by Wealth Access if such claim would not be valid but for such combination, operation, or use,

(ii) modification of any Licensed Materials, (iii) Wealth Access's compliance with Customer's designs, specifications, or instructions, or (iv) Customer's use of the Licensed Materials after Wealth Access has informed Customer of modifications or changes in the Licensed Materials required to avoid such claims if such claim would have been avoided by implementation of Wealth Access's recommended modifications and Wealth Access has offered to pay Customer's out-of-pocket costs of implementing any such modifications.

(d) EXCLUSIVE REMEDY. THE FOREGOING STATES THE ENTIRE OBLIGATION OF WEALTH ACCESS, AND THE EXCLUSIVE REMEDY OF CUSTOMER, WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS AND MISAPPROPRIATION OF TRADE SECRETS.

12. Risk Allocation.

(a) EXCLUSION OF INDIRECT DAMAGES. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY (NOR TO ANY PERSON CLAIMING RIGHTS DERIVED FROM THE OTHER PARTY'S RIGHTS) FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION LOST PROFITS, LOSS OF OR DAMAGE TO DATA, LOSS OF BUSINESS, OR OTHER ECONOMIC DAMAGE), WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND REGARDLESS OF WHETHER THE PARTY LIABLE OR ALLEGEDLY LIABLE WAS ADVISED, HAD OTHER REASON TO KNOW, SHOULD HAVE ANTICIPATED, OR IN FACT KNEW OF THE POSSIBILITY THEREOF. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS BY ANYONE. THE PROVISIONS OF THIS PARAGRAPH ARE INDEPENDENT OF, SEVERABLE FROM, AND TO BE ENFORCED INDEPENDENTLY OF ANY OTHER ENFORCEABLE OR UNENFORCEABLE PROVISION OF THIS AGREEMENT.

(b) MAXIMUM AGGREGATE LIABILITY. OTHER THAN FOR INFRINGEMENT OR MISAPPROPRIATION OF A PARTY'S INTELLECTUAL PROPERTY RIGHTS BY THE OTHER PARTY, IN NO EVENT SHALL A PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY (INCLUDING LIABILITY TO ANY PERSON OR PERSONS WHOSE CLAIM OR CLAIMS ARE BASED ON OR DERIVED FROM A RIGHT OR RIGHTS CLAIMED BY OR THROUGH SUCH PARTY), WITH RESPECT TO ANY AND ALL CLAIMS AT ANY AND ALL TIMES ARISING FROM OR RELATED TO THE SUBJECT MATTER OF THIS AGREEMENT, IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EXCEED THE FEES PAID HEREUNDER DURING THE ONE-YEAR PERIOD IMMEDIATELY PRECEDING THE ACT GIVING RISE TO CLAIM. THE PROVISIONS OF THIS PARAGRAPH ARE INDEPENDENT OF, SEVERABLE FROM, AND TO BE ENFORCED INDEPENDENTLY OF ANY OTHER ENFORCEABLE OR UNENFORCEABLE PROVISION OF THIS AGREEMENT.

(c) Intentional Risk Allocation. Each party acknowledges that the provisions of this Agreement were negotiated, as a material part of the agreement memorialized herein, to reflect an informed, voluntary allocation between them of all risks (both known and unknown) associated with the transactions involved

with this Agreement. The warranty disclaimers and limitations in this Agreement are intended, and have as their essential purpose, to limit the circumstances of liability. The remedy limitations and the limitations of liability are separately intended, and have as their essential purpose, to limit the forms of relief available to the parties.

13. Breach; Termination.

(a) Notice of Breach; Cure Period. In the event of a breach of provision of this Agreement, the notice and cure procedures set forth in this paragraph shall apply. The non-breaching party shall give the breaching party notice describing the breach and stating the time, as provided herein, within which the breach must be cured. If a provision of this Agreement sets forth a cure period for the breach in question, then that provision shall take precedence over any cure period set forth in this paragraph. No cure period shall be required, except as may be provided otherwise in this Agreement, if this Agreement sets forth specific deadline dates for the obligation allegedly breached. If the breach is (i) of an obligation to pay money or (ii) a non-willful breach of an obligation of a party relating to the other party's Confidential Information, then the breaching party shall have five business days to cure the breach after written notice thereof by the non-breaching party. If the breach is a willful breach of an obligation of a party relating to the other party's Confidential Information, then the non-breaching party, in its sole discretion, may specify in the notice of breach that no cure period will be permitted. If the breach is other than a breach of the kind described above in this paragraph, then the cure period will be 30 days after the notice of the breach by the non-breaching party.

(b) Termination for Breach. If a breach of any provision of this Agreement has not been cured at the end of the applicable cure period, if any (or upon such breach if no cure period is permitted), then the non-breaching party thereupon may terminate this Agreement by notice to the other party. This Agreement shall terminate automatically, to the extent permitted by applicable law in the jurisdiction or jurisdictions in question, if Customer makes an assignment for the benefit of its creditors, files a petition in bankruptcy, receivership, reorganization, or other like proceeding under any present or future debtor relief law (or is the subject of an involuntary such petition or filing that is not dismissed within 60 days after the effective filing date thereof), or admits of a general inability to pay its debts as they become due. Any termination of this Agreement shall be in addition to, and not in lieu of, any other rights or remedies available at law or in equity.

(c) Effect of Expiration or Termination. Upon the expiration or any termination of this Agreement, the licenses granted to Customer hereunder and all Investor Subscriptions shall terminate automatically; provided, however, that Wealth Access shall notify each Investor (by such means as Wealth Access determines, including without limitation upon such Investor's next login) of such termination and shall offer such Investor an opportunity to maintain the subscription on an individual basis in accordance with Wealth Access's then-current terms and conditions.

14. Approval of Marketing Materials; Use of Names. Customer shall not utilize any marketing materials or make any representations or statements in writing (including without limitation on a web site or in any electronic medium) regarding the Application or Wealth Access without the express prior written approval of Wealth Access, which shall not be withheld by Wealth Access unreasonably. Neither party

shall issue any press release or other publicity or marketing materials that identify the other party or the Application or use any trademark of the other party (or make any statement in any medium from which the connection of such name or mark reasonably may be inferred) without the express prior written approval of such party, which shall not be withheld by such party unreasonably. Any such approval given by a party notwithstanding, the other party shall not acquire any intellectual property rights in the names, marks, and materials of the other except for the specific use rights so approved.

15. Other Provisions.

(a) Notice. Except as otherwise expressly provided herein, notices under this Agreement shall be made in writing and shall be deemed delivered (i) when personally delivered, (ii) on the second business day after deposit when sent by certified or registered U.S. Mail, or (iii) on the next business day when sent with next-business-day instruction by recognized overnight document delivery service. Such notices shall be sent to Wealth Access at Attn: CEO, 4322 Harding Pike, Suite 417, Nashville, TN 37205, with copy to Steve Wood, Esq., Baker Donelson, 211 Commerce Street, Nashville, Tennessee 37201, and to Customer at the address shown on the Cover Page. Either party may change its address for purposes of notice by written notice thereof to the other party.

(b) Survival. The covenants herein concerning Confidential Information, indemnification, post-termination procedures, and any other provision that, by its nature, is intended to survive this Agreement shall survive any termination or expiration of this Agreement.

(c) Force Majeure. Except with respect to any payment obligations and except as otherwise expressly provided in this Agreement, neither party shall be liable for any failure to perform its obligations under this Agreement if such failure arises, directly or indirectly, out of causes reasonably beyond the direct control of such party, including without limitation acts of God, acts of terrorists or criminals, acts of domestic or foreign governments, change in any law or regulation, fires, floods, explosions, epidemics, disruptions in communications, power, or other utilities, strikes or other labor problems, riots, or unavailability of supplies.

(d) Governing Law. This Agreement shall be construed and enforced in accordance with the laws of the state of Tennessee (other than its conflicts of law provisions) and venue shall be exclusive in the federal or state courts sitting in Davidson County, Tennessee.

(e) Assignment. Customer may transfer or assign some or all of its rights and/or delegate some or all of its obligations under this Agreement only with the express prior written consent of Wealth Access, which may be granted or withheld in Wealth Access's sole discretion; provided, however, that Customer may assign all of its rights hereunder indivisibly to any Affiliate or to a purchaser of substantially all of Customer's assets so long as such assignee (i) agrees in writing to comply with Customer's obligations under, and to be bound by, this Agreement (this clause does not in itself authorize Customer to delegate its duties under this Agreement) and (ii) promptly notifies Wealth Access in writing of the same. Any purported transfer or assignment by Customer of any right under this Agreement otherwise than in accordance with the provisions of this paragraph shall be null and void and a breach of this Agreement. This Agreement shall be assignable by Wealth Access upon notice to Customer.

(f) Successors and Assigns. This Agreement will be binding upon and inure to the benefit of the parties and their successors and assigns permitted by this Agreement.

(g) Entire Agreement. Except as otherwise expressly provided herein, this Agreement constitutes the entire agreement between the parties concerning the subject matter hereof. No prior or contemporaneous representations, inducements, promises, or agreements, oral or otherwise, between the parties with reference thereto will be of any force or effect. Each party represents and warrants that, in entering into and performing its obligations under this Agreement, it does not and will not rely on any promise, inducement, or representation allegedly made by or on behalf of the other party with respect to the subject matter hereof, nor on any course of dealing or custom and usage in the trade, except as such promise, inducement, or representation may be expressly set forth herein.

(h) Amendment and Waiver. No modification or amendment to this Agreement will be valid or binding unless in writing and duly executed by the party or parties to be bound thereby. The failure of either party at any time to require performance by the other party of any provision of this Agreement shall in no way affect the right of such party to require performance of that provision. Any waiver by either party of any breach of this Agreement shall not be construed as a waiver of any continuing or succeeding breach of such provision, a waiver of the provision itself or a waiver of any right under this Agreement.

(i) Severability. If any one or more of the provisions of this Agreement should be ruled wholly or partly invalid or unenforceable by a court or other government body of competent jurisdiction, then (i) the validity and enforceability of all provisions of this Agreement not ruled to be invalid or unenforceable will be unaffected; (ii) the effect of the ruling will be limited to the jurisdiction of the court or other government body making the ruling; (iii) the provision(s) held wholly or partly invalid or unenforceable would be deemed amended, and the court or other government body is authorized to reform the provision(s), to the minimum extent necessary to render them valid and enforceable in conformity with the parties' intent as manifested herein; and (iv) if the ruling, and/or the controlling principle of law or equity leading to the ruling, subsequently is overruled, modified, or amended by legislative, judicial or administrative action, then the provision(s) in question as originally set forth in this Agreement will be deemed valid and enforceable to the maximum extent permitted by the new controlling principle of law or equity.

(j) Attorney Fees. If litigation or other action is commenced between the parties concerning any dispute arising out of or relating to this Agreement, the prevailing party will be entitled, in addition to any other award that may be made, to recover all court costs and other official costs and all reasonable expenses associated with the litigation or other action, including without limitation reasonable fees and expenses of attorneys.

(k) Injunctive Relief. Recognizing the unusual nature of computer software and trade secrets, Customer acknowledges that any violation by Customer of its covenants in this Agreement relating to Wealth Access's Confidential Information, including without limitation the Licensed Materials, would result in damage to Wealth Access that is largely intangible but nonetheless real and that is incapable of complete remedy by an award of damages. Accordingly, any such violation shall give Wealth Access the right to a

court-ordered injunction or other appropriate order to enforce specifically those covenants. Customer agrees to pay Wealth Access any reasonable expenses, including without limitation attorney fees and expenses, incurred in obtaining such specific enforcement (in addition to any other relief to which Wealth Access may be entitled).

(l) Headings. The headings of the sections used in this Agreement are included for convenience only and are not to be used in construing or interpreting this Agreement.

(m) Counterparts. This Agreement may be executed in multiple counterparts, and each manually-executed counterpart of this Agreement (whether delivered as originally executed or delivered in faxed or scanned electronic form) shall be deemed an original, all of which together shall constitute one and the same instrument. In making proof of this Agreement, it shall not be necessary to produce or account for more than one counterpart hereof signed by each of the parties.

[End of Agreement]

Yodlee: Privacy and Security FAQ

Risk Management Program

Does Yodlee have a risk management program? Yes, Yodlee has enacted a comprehensive risk management program designed to intelligently focus resources and efforts on the assessment of our corporate and information security risk profiles.

The Yodlee risk management program consists of formal risk assessments at the organizational and product level. In addition, risk management is incorporate in all facets of our processes, including integration with application development, data center operations and internal security processes. Yodlee's company-wide Enterprise Risk Management Program ensures that the necessary information is available for our Executive Management team and Board members to make effective risk-based decisions.

Information Security Program

What is Yodlee's Information Security Program? The Yodlee Information Security Program (ISP) is a comprehensive program of risk-driven polices with supporting procedures, guidelines and audit. The ISP covers all aspects of the Production, Development, Staging and Corporate environments as well as vendor relations, BCP and personnel management.

Is Management responsible for the Information Security Program? While the Yodlee culture is based on individual responsibility for security at all levels, the Yodlee Security Office (YSO) is ultimately responsible for defining, implementing and monitoring the Information Security Program. YSO operates under the supervision of the Security Oversight Committee.

What is the Yodlee Security Office (YSO)? YSO is a dedicated security function, headed by a Senior Vice President. YSO is organized around three main functions:

- Information Security

- Network Security

- Application Security

Each group is staffed with a Director, Architects and Analysts with different responsibilities relating to their primary role while also acting as backup for each other. By working closely with other Yodlee groups, YSO is able to drive security across the company.

What is the Security Oversight Committee (SOC)? The Security Oversight Committee is comprised of Executive Management and meets at least quarterly to review Yodlee's Risk Management and Information Security Programs, approve polices and to address security and risk matters.

What is Yodlee's Network Security Program? Yodlee follows industry best practice guidelines in the design and implementation of our network security environment. We use zones to separate our Production, Staging, Development, Corporate and specialty networks from each other with access control devices between each zone. We further segment networks within each zone in order to apply granular security and audit controls appropriate to each function. Other key controls include:

- Central bastion hosts
- Multi-factor authentication
- Resilient and redundant infrastructure
- Data encryption
- Centralized Security Incident and Event Management (SIEM)

What is Yodlee's Application Security Program? Security is built in our products from the specification stage and tested at multiple points up to and including release. In fact, a product cannot be released until YSO signs off. Our Application Security Program includes:

- Published secure coding standards
- Developer security training
- Manual and automated vulnerability testing
- Third-party assessments

Does Yodlee use security policies and procedures? A key component of the Yodlee Information Security Program is the policies and procedures that define our security controls. YSO is responsible for defining the policies and for working with our Operations, Customer Care and other groups to craft procedures that allow them to accomplish their tasks while protecting our customers' data. A current listing of our library is available upon request.

Does Yodlee have a Security & Privacy Awareness Program? Yodlee has integrated security and privacy awareness in all aspects of employee communications, beginning with required non-disclosure and confidentiality agreements, the setting of expectations of conduct in the employee handbook, mandatory security and privacy awareness training and testing upon hire, secure coding and build procedures, ongoing awareness programs and feedback from monitoring systems. YSO is responsible for developing, implementing and monitoring this program.

Does Yodlee have an Incident Response Program? YSO maintains Security Incident Reporting and Security Incident Response policies that define our program, as well as documented procedures that detail handling, communication and reporting to clients, regulators and law enforcement.

Independent Assessments

Does Yodlee have a SAS70 or SSAE16? Yodlee discontinued the SAS70 in favor of the BITS Shared Assessment Program. The Shared Assessment is recognized as a more comprehensive and objective assessment than a SAS70. It also tracks directly with the requirements of our clients' vendor security programs. Our assessment and the auditor's independent report are available from YSO via your Yodlee Client Partner.

Is Yodlee examined by the banking regulators? Yodlee is examined under the FFIEC Supervision of Technology Service Providers guidance. We receive a multi-agency examination, with the OCC taking the lead. For US-based financial institutions, our Report of Examination (RoE) is available from your regulator.

Is Yodlee PCI certified? Yodlee is PCI DSS certified as a Level One Service Provider. Our Report of Compliance (ROC) is available from YSO via your Yodlee Client Partner.

Personnel

Does Yodlee conduct background checks? All employee candidates, regardless of role, are subject to a thorough background investigation by YSO prior to employment. This investigation includes credit checks, criminal records search, residence verification, verification of employment and verification of academic qualifications and certifications. The Yodlee *Background Investigation Procedures* provides guidance for scoring candidates based on results and assigns a risk rating. Final approval for candidates is given by YSO.

Do employees sign confidentiality agreements? Employee candidates sign non-disclosure agreements prior to hiring. These are executed on the candidate's first visit or when discussions are initiated. A second Employee NDA is signed when an individual is hired.

Is there a formal termination procedure? Formal procedures for employee separation are defined to coordinate the applicable tasks between HR, YSO and the Yodlee IT department. The procedures define protocols for scheduled and immediate terminations.

Physical Security

How is site security handled at Yodlee? Physical security is also managed by YSO and is taken quite seriously. At our offices, all employees must have and display their HID badge at all times. There are strict rules against tailgating. All visitors must present themselves at Reception to sign in and receive a Visitors Badge. Visitors are escorted while on the site at all times and must surrender their badge when they leave. Access to sensitive areas requires YSO approval based on job responsibility. The most sensitive areas have biometric access devices used in tandem with the HID badge reader.

At our Data Centers, access is only granted to necessary Operations and YSO personnel, who must be pre-approved by YSO. Access to the data centers requires badge and biometric identification. Visitors to the Data Center must be accompanied by an authorized Yodlee employee, must sign in and surrender a government-issued photo ID while on site. All Yodlee facilities have comprehensive video surveillance.

Vendor Management

How are critical vendors managed? Yodlee's Vendor Management Program is used to ensure that our service providers are selected and managed using risk-based criteria appropriate to their role. These criteria range include financial due diligence, security assessments and onsite visits. Vendors are reviewed at least annually, with ongoing management activities for our most critical service providers.

Business Continuity Program

Does Yodlee have a BCP? Yodlee has a formal Business Continuity Program that encompasses all functions and sites. We conduct Business Impact Analyses upon significant changes to our environment or personnel, but at least annually.

Does Yodlee test their BCP? We conduct a variety of tests through-out the year to ensure that our BCP is designed and operating effectively.

Does Yodlee consider pandemic planning as part of their BCP? Pandemic planning has been part of our BCP since 2006 and is updated to track with current pandemic threats.

Disaster Recovery Services

Is Disaster Recovery part of Yodlee's services? Yodlee has formal DR programs for our internal services and our clients' applications. Our client DR options included contracted RPO and RTO designed to map with our client's requirements. More information is available from your Yodlee Client Partner.

Does Yodlee test their DR plan? Yodlee conducts regular tests of our internal DR and requires annual testing with clients of their DR option.

Development and Change Control

Does Yodlee follow a formal SDLC? The Yodlee Unified Process (YUP) is our formal software development framework. It is a hybrid methodology, based on agile practices, that allows us to define, develop, test and release our products in a secure and timely manner. More information is available from your Yodlee Client Partner.

How does Yodlee perform Change Management? The Yodlee Change Management (YCM) program is a formal and rigorous ITIL-based methodology for requesting, testing, approving and promoting changes to our Production Environment. More information is available from your Yodlee Client Partner.

[End of Agreement]

byallaccounts: Security & Privacy

Available at http://www.byallaccounts.com/what_we_do/security_privacy.html

Our data aggregation technology captures and manages highly sensitive financial information. We place great emphasis on safeguarding this information and maintaining a high level of security around it. We employ industry-leading technologies and policies to protect the confidentiality and privacy of each user's financial and personal data. We vigilantly update our systems to stay at the forefront of security, privacy and continuity protection.

At ByAllAccounts, we have created a high-security environment designed to insure the privacy and security of its clients and their data. To assure this security, we employ a number of different technologies including:

Network security

Application security

Encryption

All personal user information is stored in an encrypted format in the ByAllAccounts database, and is transmitted in that encrypted format within the network.

Production systems are run on dedicated equipment housed in a SAS70 Type II certified environment at SunGard Availability Services. The environment includes state-of-the-art security, redundant power, redundant high-speed Internet connections, system monitoring and management, comprehensive backup, and disaster recovery.

We perform extensive security checks on our employees and have implemented stringent internal controls with regard to sensitive information.

Our security and privacy policies and procedures are reviewed by independent auditors on a periodic basis. In addition, we keep access logs and other historical information to provide clear audit trails. It is important to note that as part of the overall security process, we do not publicly provide specific details regarding our security procedures and processes. We would be happy to discuss any questions or concerns regarding our security, backup, or disaster recovery plans and processes or the security vendors we employ.

BITS Voluntary Guidelines for Aggregation

ByAllAccounts complies with the BITS Voluntary Guidelines for Aggregation. BITS, the Technology Group for The Financial Services Roundtable, was formed in 1996 by Spencer Eccles, chairman of Wells Fargo and Terrence Murray, Chief Executive Officer of the FleetBoston Financial Corporation. The membership includes CEOs of the largest bank-holding institutions in the United States. The BITS organization serves as the strategic "brain trust" for the financial services industry in the e-commerce arena.

The BITS Aggregation Services initiative's goal is to create a more secure operating model for aggregation and to create industry options and recommendations for a cooperative approach to data feeds

and authentication. Technology providers, such as ByAllAccounts, government regulators and financial institutions regularly participate as members of the Aggregation Services Working Group. Participants generally include senior executives involved with aggregation services, activities, policies or business practices.

ByAllAccounts has reviewed the BITS Voluntary Guidelines for Financial Services that set forth best practices for security, privacy and consumer education in aggregation services and is in substantial compliance with these guidelines.

SAS 70

SAS 70 - Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). An SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

[End of Agreement]

Amazon Web Services: Security and Privacy

Overview

At a high level, we've taken the following approach to secure the AWS infrastructure:

- **Reports, Certifications, and Independent Attestations.** AWS has in the past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards as well as a Service Organization Controls 2 (SOC 2) report. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP). We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services. For more information on risk and compliance activities in the AWS cloud, consult the [Amazon Web Services: Risk and Compliance](#) whitepaper.
- **Physical Security.** Amazon has many years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secured with a variety of physical controls to prevent unauthorized access.
- **Secure Services.** Each of the services within the AWS cloud is architected to be secure and contains a number of capabilities that restrict unauthorized access or usage without sacrificing the flexibility that customers demand. For more information about the security capabilities of each service in the AWS cloud, consult the [Amazon Web Services: Overview of Security Processes](#) whitepaper.
- **Data Privacy.** AWS enables users to encrypt their personal or business data within the AWS cloud and publishes backup and redundancy procedures for services so that customers can gain greater understanding of how their data flows throughout AWS. For more information on the data privacy and backup procedures for each service in the AWS cloud, consult the [Amazon Web Services: Overview of Security Processes](#) whitepaper referenced above.

The AWS Security Center provides links to technical information, tools, and prescriptive guidance designed to help you build and manage secure applications in the AWS cloud. Our goal is to use this forum to proactively notify developers about security bulletins. Such transparency is the backbone of trust between AWS and our customers.

Certifications and Accreditations

SOC 1/SSAE 16/ISAE 3402

Amazon Web Services now publishes a Service Organization Controls 1 (SOC 1), Type 2 report. The audit for this report is conducted in accordance with the Statement on Standards for

Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. Our commitment to the SOC 1 report is on-going and we plan to continue our process of periodic audits. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report.

SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type 2 report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting customer data.

FISMA Moderate

AWS enables U.S. government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). FISMA requires federal agencies to develop, document, and implement an information security system for its data and infrastructure based on the National Institute of Standards and Technology Special Publication 800-53, Revision 3 standard. FISMA Moderate Authorization and Accreditation requires AWS to implement and operate an extensive set of security configurations and controls. This includes documenting the management, operational, and technical processes used to secure the physical and virtual infrastructure, as well as the third-party audit of the established processes and controls. AWS has received a three-year FISMA Moderate authorization for Infrastructure as a Service from the General Services Administration. AWS has also successfully achieved other ATOs at the FISMA Moderate level by working with government agencies to certify their applications and workloads.

PCI DSS Level 1

AWS has achieved Level 1 PCI compliance. We have been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Merchants and other service providers can now run their applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. Other enterprises can also benefit by running their applications on other PCI-compliant technology infrastructure. PCI validated services include Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Elastic Block Storage (EBS) and Amazon Virtual

Private Cloud (VPC), Amazon Relational Database Service (RDS), Amazon Elastic Load Balancing (ELB), Amazon Identity and Access Management (IAM), and the underlying physical infrastructure and the AWS Management Environment.

For more information please visit our [PCI DSS Level 1 FAQs](#).

ISO 27001



Registered organization (N° 2018-002) AWS has achieved [ISO 27001 certification](#) of our Information Security Management System (ISMS) covering our infrastructure, data centers, and services including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) and Amazon Virtual Private Cloud (Amazon VPC). ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing transparency into our security controls and practices. AWS's ISO 27001 certification includes all AWS data centers in all regions worldwide and AWS has established a formal program to maintain the certification. A copy of our ISO certificate, available to AWS customers, describes the ISMS services and geographic scope.

For more information please visit our [ISO 27001 FAQs](#).

International Traffic In Arms Compliance

The AWS GovCloud (US) region supports US International Traffic in Arms Regulations (ITAR) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to US land. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data under ITAR. The AWS GovCloud (US) environment has been audited by an independent third party to validate the proper controls are in place to support customer export compliance programs for this requirement.


FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL terminations in AWS GovCloud (US) operate using FIPS

140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance when using the AWS GovCloud (US) environment.

Other Compliance Initiatives





The flexibility and customer control that the AWS platform provides permits the deployment of solutions that meet industry-specific compliance requirements.

- **HIPAA:** Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules  on AWS. AWS provides the security controls customers can use to help to secure electronic health records. Please see the related whitepaper (link below).
- **CSA:** AWS has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire. This questionnaire published by the CSA provides a way to reference and document what security controls exist in AWS's Infrastructure as a Service offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Customers can find the completed questionnaire in Appendix A of the AWS Risk and Compliance whitepaper
- **MPAA:** The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. Media companies use these best practices as a way to assess risk and audit their content and infrastructure. AWS commissioned an independent assessment of AWS's compliance with the MPAA best practices and has achieved the highest maturity rating possible, indicating that the AWS infrastructure is compliant with all applicable MPAA infrastructure controls across all the AWS services under review. While the MPAA does not offer a "certification", media companies can use this report to complete their own risk assessment and audit of MPAA-type content on AWS.

[↑ Top](#)

Background Information

Delivering a secure cloud computing platform involves implementing numerous best practices for on-premise infrastructure as well as a host of additional considerations unique to a hosted infrastructure environment. The Amazon Web Services: Overview of Security Processes whitepaper will provide background information and an overview of the AWS philosophy in offering a secure cloud computing platform.

-  **Amazon Web Services Overview of Security Processes whitepaper** (pdf)
-  **Security Best Practices** (pdf)
-  **Creating HIPAA-Compliant Medical Data Applications with AWS whitepaper** (pdf)
-  **AWS Risk and Compliance whitepaper** (pdf)

Security Features

AWS provides a number of ways for you to identify yourself and securely access your AWS account, the AWS services you have signed up for, and the resources hosted by these services. You can find the complete list of credentials that we support on the [Security Credentials](#) page under *Your Account*. We also provide additional security options that enable you to further protect your AWS account and control access: Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and Key Rotation.

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) enables you to create multiple Users and manage the permissions for each User within your AWS Account. A *User* is an identity (within a customer AWS Account) with unique security credentials that can be used to access AWS resources. IAM eliminates the need to share passwords or access keys and makes it easy to enable or disable a User's access as appropriate.

IAM enables you to implement security best practices, such as least privilege, by assigning unique credentials to every User within your AWS Account and granting only the permissions Users need to access the AWS resources required for them to perform their jobs. IAM is secure by default; new Users have no access to AWS until permissions are explicitly granted.

IAM allows you to minimize the use of your AWS Account credentials. Instead, all interactions with AWS resources should occur in the context of IAM User security credentials. To learn more about AWS Identity and Access Management (IAM) [visit our IAM page](#).

AWS Multi-Factor Authentication (AWS MFA)

AWS Multi-Factor Authentication (AWS MFA) is an additional layer of security that offers enhanced control over your AWS Account settings and the management of the AWS resources to which the account has subscribed. When you enable this opt-in feature, you'll need to provide a six-digit single-use code in addition to your standard user name and password credentials before access is granted. You get this single use code from an authentication device or a special application on a mobile phone that you keep in your physical possession. This is called Multi-Factor Authentication because two factors are checked before access is granted to your account: you need to provide both your AWS email ID and password (the first "factor": something you know) *and* the particular code from your authentication device (the second "factor": something you have). Multi-Factor Authentication can be enabled for your AWS Account as well as for the Users you have created under your AWS Account using IAM.

It is easy to obtain an authentication device from a participating third party provider, or download and install appropriate software on your mobile phone, then set it up for use via the AWS website. More information about Multi-Factor Authentication is available [here](#).

Key Rotation

For the same reasons as it is important to change your password frequently, AWS recommends that you rotate your access keys and certificates on a regular basis. To let you do this without potential impact to your applications' availability, AWS supports multiple concurrent access keys and certificates. With this feature, you can rotate keys and certificates into and out of operation on a regular basis without any downtime to your application. This can help to mitigate risk from lost or compromised access keys or certificates. The IAM APIs enable you to rotate the access keys of your AWS Account as well as for Users created under your AWS Account.

To learn more about this feature or to begin using key rotation, [click here](#).

[↑ Top](#)

AWS Public PGP Key

The AWS Security Team encourages customer communication. We have established processes for [reporting security vulnerabilities](#) and for [requesting penetration testing](#). We have also created a [signed PGP key](#) for especially sensitive communications you may need to send.

[End of Agreement]